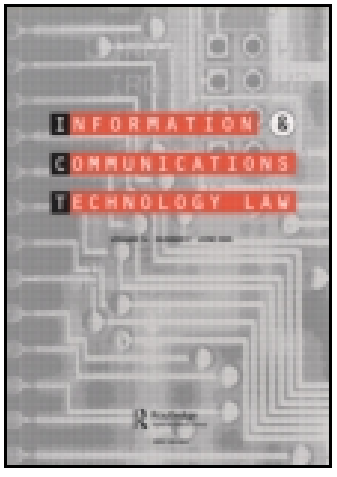

Information & Communications Technology Law
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/cict20

Social media and our misconceptions of the realities

Richard Sanvenero[a]
[a] School of Law, Barry University, Orlando, FL, USA
Published online: 28 Aug 2013.

To cite this article: Richard Sanvenero (2013) Social media and our misconceptions of the realities, Information & Communications Technology Law, 22:2, 89-108, DOI: 10.1080/13600834.2013.805923

To link to this article: http://dx.doi.org/10.1080/13600834.2013.805923

Information & Communications Technology Law, 2013
Vol. 22, No. 2, 89–108, http://dx.doi.org/10.1080/13600834.2013.805923

Social media and our misconceptions of the realities

Richard Sanvenero*

School of Law, Barry University, Orlando, FL, USA

This article will review the current laws of the expectations of privacy under the two-pronged Katz test, and more specifically other cases that the courts have tried to interpret the test as applicable to social media such as Facebook, Instagram, Twitter, and email. Since there seems to be 'no light at the end of the tunnel' with any uniform decision within the courts on the Fourth Amendment protections against search and seizure when there is a reasonable expectation of privacy with social media. This reasonable expectation standard is developed by the users themselves who will allow their rights to be infringed upon for the approval to access sites like Facebook, Twitter, and Instagram.

Keywords: Facebook; Twitter; email; Instagram; Fourth Amendment; social media; Katz test

1. Introduction

Social Media has furthered changes in our everyday life since the early 2000s. This claim is based on changes within our cultured society by the interactions of comments or liking pictures and sharing ideas. The Fourth Amendment states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[1]

Since there seems to be 'no light at the end of the tunnel' with any uniform decision within the courts on the Fourth Amendment protections against search and seizure when there is a reasonable expectation of privacy with social media. This reasonable expectation standard is developed by the users themselves who will allow their rights to be infringed upon for the approval to access sites like Facebook and Instagram. This article will review the current laws of the expectations of privacy under the two-pronged *Katz* test, and more specifically other cases that the courts have tried to interpret the test as applicable to social media.[2]

The Social Media epidemic is not just limited to an Internet accessible computer. Now social media sites have taken over many aspects by the creation of digital applications ('app') (Campbell, 2011) that can be downloaded to a tablet,[3] smartphone,[4] or PDA.[5] The most popular social media apps currently available for download are Facebook,

*Email: richard.sanvenero@law.barry.edu

Twitter, and Instagram (Smith, 2009). In a way, it has furthered a technological change from basic emailing to more of a social media interaction. The purpose of this article will focus on court decisions and lawsuits that have came due specifically to the Internet of email or social media. The false hope to come out of this article, would bring awareness to the public over how technology can pave the way decisions are made in the judicial system today.

2. The evolution of Facebook and the policy changes

The cyber world exploded in the late 1990s with Microsoft's creation of the Internet Explorer, a search engine that allowed windows computer users to access any existing website, by using a website address.[6] The Internet in the 1990s was primarily used for Web browsing and Internet Service Provider email services. The Internet world today has been infected with a disease called social media. Social media is designed to be disseminated through social interaction, created using highly accessible and scalable publishing techniques.[7] Social media was created by the Internet, which allows people to exchange personal information with one another. Facebook is the biggest social media website of them all, started in 2004 by Mark Zuckerberg. Originally, Facebook was used as a closed social network that required registration with a university email address from an Ivy League school. Slowly, Facebook became open to all schools. Its initial exclusivity undoubtedly contributes to its publicity and popularity. By 2006, when the site was opened to the general public, 'its club like, ritualistic, highly regulated foundation was already in place' (Semitsu, 2011). This idea of sharing information from a person's profile to another profile was ingenious and very addicting to many users of Facebook across the world. The total number of Facebook users today exceeds the one billion mark, although, the members of Facebook are not all 'daily active users'.[8]

To sign up to Facebook, you are required to provide information such as your name, email address, birthday, and gender. In some cases, you may be able to register using other information, like your telephone number.[9] Before an account is created, you as the user must agree to Facebook's Terms, Data Use Policy, and Cookie Use.[10] After all of the terms have been agreed upon, then you are an official user of Facebook. The terms-of-service agreement is mainly used for legal purposes by websites and Internet Service Providers that store a user's personal data, such as e-commerce and social networking services. A legitimate terms-of-service agreement is legally binding, and may be subject to change.[11]

The Facebook user agreements have vastly changed over the course of its existence. Since 2005, Facebook has seen many changes in its user agreements. In 2005, Facebook's policy stated '[n]o personal information that you submit to Facebook will be available to any user of the Web Site who does not belong to at least one of the groups specified by you in your privacy settings' (Semitsu, 2011, p. 302). Two years later, the language again was changed and replaced with:

> Profile information you submit to Facebook will be available to users of Facebook who belong to at least one of the networks you allow to access the information through your privacy settings (e.g., school, geography, friends of friends). Your name, school name, and profile picture thumbnail will be available in search results across the Facebook network unless you alter your privacy settings. (Semitsu, 2011, p. 303)

All of this information that Facebook collects is then disseminated and send to about five hundred thousand third-party application developers.[12]

By 2009, the categories of information were expanded and available to everyone by default (Semitsu, 2011, p. 303). This 2009 privacy policy was longer than the United States Constitution without any of its amendments (Bilton, 2010).[13] Again in 2010, the policy was changed to reflect Facebook's thought process of sharing your information with third parties that they deemed would have been permitted by you, reasonably necessary to offer our services, or when legally required to do so (Semitsu, 2011, p. 305). In 2010, another change to the Facebook added privacy controls and streamlined its privacy settings, giving users more ways to manage status updates and other information that is broadcast to the public News Feed.[14] Among the new privacy settings is the ability to control who sees each new status update a user posts: Everyone, Friends of Friends, or Friends Only.[15] Users can now hide each status update from specific people as well.[16] However, a user who presses 'like' or comments on the photo or status update of a friend cannot prevent that action from appearing in the news feeds of all the users' friends, even non-mutual ones.[17]

The latest policy change occurred on 11 December 2012, making Facebook similar to an old school tyrant, exploiting its users, increased complexity, and violation of privacy in the context of the processing of sensitive personal data.[18] The new privacy policy does not have any surprises in the context of targeted advertising: Just like the old policy, it legitimates the use of profile data, browsing data, social network data for the purpose of targeting ads, a practice that means that the user data is not their own, (i.e. work without payment for producing a data commodity that is sold to advertisers).[19] Advertisers then present ads to users: '[s]ometimes we get data from our affiliates or our advertising partners, customers and other third parties that helps us (or them) deliver ads, understand online activity, and generally make Facebook better'.[20]

For example, an advertiser may tell us information about you (like how you responded to an ad on Facebook or on another site) in order to measure the effectiveness of – and improve the quality of – ads.[21]

> We use the information we receive, including the information you provide at registration or add to your account or timeline, to deliver ads and to make them more relevant to you. This includes all of the things you share and do on Facebook, such as the pages you like or key words from your stories, and the things we infer from your use of Facebook.[22]

When an advertiser creates an ad, they are given the opportunity to choose their audience by location, demographics, likes, keywords, and any other information we receive or can tell about you and other users.[23] For example, an advertiser can choose to target 35–55-year-old men who live in the USA and like golf. An advertiser could also choose to target certain topics or keywords, like 'golf' or even people who like a particular event or golfer.[24] Facebook exploits the its users to advertisers by allowing them to target a category of user, like a 'baseball player' or a 'baseball fan'. We do this by bundling characteristics that we believe are related to the category.

For example, if a person 'likes' the 'New York Yankees' page and mentions 'Derek Jeter' when they check into a baseball field, we may conclude that this person is likely to be a New York Yankee fan. Advertisers of baseball, for example, could ask us to target 'baseball fans' and we would target that group, which may include you. Or if you 'like' pages that are 'video game' based and mention a particular video game system in a post, we might put you in the video game category and let a video game company target to that group, which would include you.[25]

Another change in the privacy policy is the addition to 'personalized ads'. 'If you indicate that you are interested in topics, such as by liking a page, including topics such

as products, brands, religion, health status, or political views, you may see ads related to those topics as well.'[26] Additionally Facebook states '[w]e may disclose information pursuant to subpoenas, court orders, or other requests (including criminal and civil matters) if we have a good faith belief that the response is required by law'. It 'may' respond to mere government 'requests', suggests a standard far lower than reasonable suspicion or probable cause. The 'required by law' part of the first sentence might be interpreted to mean that it will deny any 'requests' unless it will face obstruction or contempt charges. What does 'required by law' mean to Facebook? That becomes an undefined standard that requires either legislative or judicial action. Facebook finishes their privacy policy off with a final disclaimer stating:

> We may also share information when we have a good faith belief it is necessary to prevent fraud or other illegal activity, to prevent imminent bodily harm, or to protect ourselves and you from people violating our Statement of Rights and Responsibilities. This may include sharing information with other companies, lawyers, courts or other government entities.[27]

3. Uproar over Instagram

Instagram is an online photo-sharing and social networking service that enables its users to take pictures, apply digital filters to them, and share them on a variety of social networking services, such as media sites including Facebook or Twitter (Frommer, 2010). Instagram has exploded over the past few years with the development of smartphone technology, allowing Instagram users to post pictures with edited effects, from their supported smartphone to their Instagram account. This service has been very popular. Facebook recently purchased Instagram for $1 billion dollars in 2012 (Culter, 2012). Over the course of its birth since 2010, it has eclipsed a million users in the first three months.[28]

The Terms of Use were less confusing in 2010, stating requirements of

- being at least 13 years old to use the Service.
- You may not post violent, nude, partially nude, discriminatory, unlawful, infringing, hateful, pornographic or sexually suggestive photos or other content via the Service.
- You agree that you will not solicit, collect or use the login credentials of other Instagram users.
- You are responsible for keeping your password secret and secure.
- You must not defame, stalk, bully, abuse, harass, threaten, impersonate or intimidate people or entities and you must not post private or confidential information via the Service, including, without limitation, your or any other person's credit card information, social security or alternate national identity numbers, non-public phone numbers or non-public email addresses.[29]

The Terms of Use were updated again in December 2012, stating a controversial clause stated:

> you agree that a business or other entity may pay us to display your username, likeness, photos (along with any associated metadata), and/or actions you take, in connection with paid or sponsored content or promotions, without any compensation to you. (Pepitone, 2012)

There was no apparent option to opt-out of the changed terms of use.[30]

Some Rights were also revised such as

> Instagram does not claim ownership of any Content that you post on or through the Service. Instead, you hereby grant to Instagram a non-exclusive, fully paid and royalty-free, transferable, sub-licensable, worldwide license to use the Content that you post on or through the Service, subject to the Service's Privacy Policy, available here http://instagram.com/legal/privacy/, including but not limited to sections 3 ('Sharing of Your Information'), 4 ('How We Store Your Information'), and 5 ('Your Choices About Your Information'). You can choose who can view your Content and activities, including your photos, as described in the Privacy Policy. Some of the Service is supported by advertising revenue and may display advertisements and promotions, and you hereby agree that Instagram may place such advertising and promotions on the Service or on, about, or in conjunction with your Content. The manner, mode and extent of such advertising and promotions are subject to change without specific notice to you.[31]

We wonder, 'do we actually own our pictures and comments on Instagram?' In this case, the co-creator Kevin Systrom of Instagram came out with a statement after the uproar over the 2012 changed Terms of Use. Kevin stated,

> Earlier this week, we introduced a set of updates to our privacy policy and terms of service to help our users better understand our service. In the days since, it became clear that we failed to fulfill what I consider one of our most important responsibilities – to communicate our intentions clearly. I am sorry for that, and I am focused on making it right. The concerns we heard about from you the most focused on advertising, and what our changes might mean for you and your photos. There was confusion and real concern about what our possible advertising products could look like and how they would work. Because of the feedback we have heard from you, we are reverting this advertising section to the original version that has been in effect since we launched the service in October 2010. You can see the updated terms here. Going forward, rather than obtain permission from you to introduce possible advertising products we have not yet developed, we are going to take the time to complete our plans, and then come back to our users and explain how we would like for our advertising business to work. You also had deep concerns about whether under our new terms, Instagram had any plans to sell your content. I want to be really clear: Instagram has no intention of selling your photos, and we never did. We don't own your photos – you do.[32]

The statement by Kevin would infer to the reasonable person that Instagram does not own your pictures to sell to third party ad companies. The collective users of Instagram uprising against the policy change caused a public statement to be made. This may be the first of many social media uprisings to come over the infringements on our rights of privacy.

3.1 *#Twitter #attacks Instagram over policy changes*

A number of celebrities have come out on their Twitter[33] accounts after Instagrams' new Terms of Service (Hernandez, 2012). Celebrities such as: Anderson Cooper, Pink, Sophia Bush, DeadMau5, Owl City, and Nina Garcia have tweeted about their frustration about Instagram.[34] Even Deadmau5 tweeted 'Here you go Instagram, feel free to sell this posted photo for cash. Thanks for selling me out. #instagram.'[35] The photo posted by Deadmau5 himself, involved him 'flipping the bird' to Instagram.[36]

4. Where it all began with the 'Katz test'

The landmark Supreme Court ruling in *Katz* v. *United States* sets out the nature of the 'right of privacy' and what considers to be a 'search'.[37] Katz was charged with transmitting

wagering information by telephone from Los Angeles to Miami and Boston, in violation of a federal statute.[38] The Government introduced evidence of Katz telephone conversation, overheard by an electronic listening recording device by the FBI outside the public phone booth he called from.[39] The Court's ruling has adopted the unreasonable search and seizure clause of the Fourth Amendment protections to all areas where a person has a 'reasonable expectation of privacy'.[40] When dealing with searches, the *Katz* Court has decided that wiretapping counts as a search, not making physical intrusions necessary.[41] Justice Harlan's concurring opinion in *Katz* has transformed later courts decisions by his two-pronged test.[42] The two pronged of the test for determination of the existence of privacy by (1) the person 'have exhibited an actual (subjective) expectation of privacy' and (2) the expectation be one that society is prepared to recognize as 'reasonable'.[43]

The majority in *Katz* decided instead that the legal issue was whether Katz knowingly exposed information to the public or attempted to keep the information private.[44] The Court decided here 'the Fourth Amendment protects people, not places'.[45] What a person knowingly exposes to the public, even in his own home or office, is not subject to Fourth Amendment protection.[46] 'But what he seeks to preserve as private, even in an area accessible to the public may be constitutionally protected.'[47] The reasonableness requirement is set forth in a two-fold requirement:

> First that a person [has] *exhibited* an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable'. Thus a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the 'plain view' of outsiders are not 'protected' because no intention to keep them to himself has been exhibited. On the other hand conversations in the open would not protected against being overheard, for expectation of privacy under the circumstances would be unreasonable.[48]

Later the Supreme Court decisions have used Justice Harlan's two-pronged test of the government engaging in a search where the suspect had a 'reasonable expectation of privacy'.[49] Leading into the *Smith* v. *Maryland*, the Court focused on the subjective prong of the two-pronged test with the majority's vague privacy focus stating, '[t]he first [prong] is whether the individual, by his conduct has "exhibited" an actual (subjective) "expectation of privacy", whether, in words of the *Katz* majority, the individual has shown that "he seeks to preserve [something] as private"'.[50] In order for the individual to claim these protections he must show *through his conduct* that he attempted to protect something as private.

4.1 *The two-pronged test complexity*

Concern had arisen in a short few years from the *Katz* ruling, in which Justice Harlan expressed concern about the application of his two-pronged test in his dissent in *United States* v. *White*.[51]

In *White*, an employed police informant wore a device that transmitted to the government agents his conversations with White, which had occurred in the informant's home and car, White's home, and a restaurant.[52] During the trial, the government could not locate the informant to testify, and the agents who conducted the surveillance testified as to the conversations.[53] The plurality opinion held that White by the evidence admitted, had assumed the risk that the person in who he confided was either not an informant, or an informant with a transmitter.[54] The Court found that the agents had not violated any legitimate expectation of privacy when the informant transmitted and agents monitored the conversations.

Justice Harlan challenged the plurality's position that there was no distinction between agents monitoring conversations and undercover informants participating in their conversations. He stated:

> The force of the contention [that there is no distinction] depends on the evaluation of two separable but intertwined assumptions: first, that there is no greater of invasion of privacy in the third-party situation, and, second, that uncontrolled consensual surveillance in an electronic age is a tolerable technique of law enforcement, given the values and goals of our political system.[55]

It seems Justice Harlan is questioning the applicability. Reciting his approach in *Katz* may have 'misconceived' the true concern of the Fourth Amendment by focusing incorrectly on the individual, rather than the impact of the practice on the whole of society.[56]

Justice Harlan raises an alternative as to when the two-pronged test fails. The Court by engaging in the analysis of 'examining the desirability of saddling [such expectations] upon society'.[57] Justice Harlan further proposes the use of a balancing test of '[1] assessing the nature of a particular practice and [2] the likely extent of its impact on the individual's sense of security [3] balanced against the utility of the conduct as a technique of law enforcement'.[58]

> Whether privacy expectations are legitimate within the meaning of *Katz* depends not on the risks an individual can be presumed to accept when imparting information to third parties, but on the risks he should be forced to assume in free and open society. By its terms, the constitutional prohibition of unreasonable searches and seizures assigns to its judiciary some prescriptive responsibility.[59]

This becomes more of an objective standard of an approach of what society will approve. Harlan goes on to further state '[the] critical question, therefore is whether under our system of government, as reflected in the Constitution, we *should* impose on our citizens the risks of the electronic listener or observer without at least the protection of a warrant requirement' (Hancock, 2009). Justice Blackmun later acknowledged Justice Harlan's cautionary note in his *White* dissent, Justices Marshall and Brennan explicitly embraced Harlan's fundamental approach to 'evaluate the "intrinsic character" of investigative practices with reference to the basic values underlying the Fourth Amendment'.[60]

In *Smith*, it dealt with a request from law enforcement agents to the telephone company to install a device that records outgoing phone numbers dialed from Smith's home, but not the content of the ensuing conversations.[61] The Court upheld this warrantless search because it found that Smith had no reasonable expectation of privacy in the phone numbers dialed due to his awareness of the numbers' exposure to the phone company.[62] This allowed the Court to recognize situations in which the two-pronged test would not be applicable. The Court stated: '[s]ituations can be imagined, of course, in which *Katz's* two-pronged inquiry would provide an inadequate index of Fourth Amendment protection'.[63]

> For example, if the Government were suddenly to announce on nationwide television that all homes henceforth would be subject to warrantless entry, individuals thereafter might not in fact entertain any actual expectation of privacy regarding their homes, papers, and effects. Similarly, if a refugee from a totalitarian country, unaware of this Nation's traditions, erroneously assumed that police were continuously monitoring his telephone conversations, a subjective expectation of privacy regarding the contents of his calls might be lacking as well. In such

> circumstances, where an individual's subjective expectations has been 'conditioned' by influences alien to well-recognized Fourth Amendment freedoms, those subjective expectations obviously could play no meaningful role in ascertaining what the scope of Fourth Amendment protection was. In determining whether a 'legitimate expectation of privacy' existed in such cases, a normative inquiry would be proper.[64]

The Court carefully approached this because it cautioned that the government could not limit privacy expectations by merely stating its intention to spy on its citizens: if the government did so, the expectation-of-privacy test would be inadequate, and a 'normative' inquiry would be necessary.[65] The Court has continued to apply the two-pronged test in *Katz*.[66] Flaws have been pointed out to this approach under certain circumstances or, as Justice Scalia puts it, 'all circumstances'.[67]

5. Electronic Communications Privacy Act 1986

The Electronic Communications Privacy Act 1986 ('Privacy Act') was created to update the Federal Wiretap Act of 1968, which addressed concerns originating over wiretapping. The Privacy Act now includes computers and other digital and electronic communication. The Privacy Act 'protects wire, oral, and electronic communications while those communications are being made, are in transit, and when they are stored on computers'.[68] The Act applies to email, telephone conversations, and data stored electronically. The Privacy Act takes a general approach of 'providing greater privacy protection for materials in which there are greater privacy interests'.[69] The Privacy Act is broken down into three sections.

The first section of the Privacy Act is referred to as the Wiretap Act, prohibits the intentional actual or attempted interception, use, disclosure, or 'procure[ment] [of] any other person to intercept or endeavor to intercept any wire, oral, or electronic communication'.[70] It provides exceptions for operators and service providers for uses 'in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service' and for 'persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance'.[71] It sets out procedures for 'Federal, State, and other government officers to obtain judicial authorization for intercepting such communications, and regulates the use and disclosure of information obtained through authorized wiretapping.'[72]

The second section of the Privacy Act became known as the Stored Communications Act (SCA).[73] It protects against the 'privacy of the contents of files stored by service providers and of records held about the subscriber by service providers, such as the subscriber's name, billing records, or IP addresses'.[74]

The third section of the Privacy Act addresses the pen register, and traps and trace devices, requiring government entities to obtain a court order.[75] The court order must authorize the installation and use of a pen register[76] and/or a trap and trace device.[77] No actual communications are intercepted by a pen register or trap and trace.[78] The authorization order can be issued on the basis of certification by the applicant, finding that the information to be obtained is relevant to an ongoing criminal investigation, being conducted by the applicant's agency.[79]

6. Should Facebook be considered privacy friendly?

Facebook is not known to be privacy friendly with their users information to the outside world (Cranor, 2009). Facebook is known to be a popular social network, where

members develop a personalized web profile to interact and share information with other members.[80] The information that is shared on Facebook can include things such as: news headlines, photographs, videos, personal stories, and activity updates.[81] Any of these things are generally published from a Facebook account that will be broadcasted to the members' online 'friends'.[82] The more we share as 'users' of Facebook, the more valuable Facebook as a network becomes to advertisers and marketers (Purewal, 2011).

In 2007, Facebook created a program called 'Beacon', which would allow Facebook members to share with their 'friends', information about where else on the Internet they have visited.[83] Beacon would update the members profile to reflect certain actions the member had taken on websites belonging to companies that had contracted with Facebook to participate in the Beacon program. For example, visiting a website like Blockbuster.com that participates in the Beacon program would in turn transmit any data regarding rentals to Facebook, and Facebook would then broadcast that information to everyone in the member's online network by posting the data to their personal profile. The issue with the Beacon program was that it never acquired the affirmative consent of the users of Facebook to publish these events on their behalf.[84] To opt-out of the Beacon program required video game skills by actively opting out.[85]

Again in 2011, Facebook announced it would implement 'Facial recognition technology', which allows Facebook to suggest tags to your friends of pictures they upload of you (Purewal, 2011). This seems harmless at first, but over time it is infringing on your privacy rights by allowing Facebook to create the ability to search for people by using just a picture.[86] With more and more pictures posted to Facebook over time, Facebook can literally create a profile of you from your images. Does this sound creepy?

Since Facebook relies on advertisers and marketers to fund the website, it created new levels of advertising in 2011 through 'Sponsored Stories'.[87] User activity on Facebook has been the fuel for 'sponsored stories'.[88] Advertisers pay to highlight an action that users have already taken on the Facebook or within a Facebook-connected app. This action by the user, is then displayed to the user's approved friends, either in the sidebar or in News Feed by using the user names' and profile picture who clicked 'like'.[89] There is no option to opt-out of 'Sponsored Stories' from using your name or picture in their advertisement.[90]

A class action lawsuit *Fraley* v. *Facebook, Inc.*, has been filed against Facebook, Inc., claiming that Facebook unlawfully used Class Members' names, profile pictures, photographs, likenesses, and identities to advertise or sell products and services through Sponsored Stories, without obtaining Class Members' consent.[91] Facebook relies on their provisions of the Privacy Policy of the Statement of Rights and Responsibilities stating, '[y]ou give us permission to use your name and Facebook profile picture in connection with [commercial, sponsored, or related] content, subject to the limits you place'.[92]

The Fraley court relied on the California Civil Code §3344, which prohibited the non-consensual use of another's name, voice, signature, photograph, or likeness for advertising, selling, or soliciting purposes, and creates a cause of action for persons injured by such actions.[93] 'California law provides two vehicles for asserting such a right: a common law cause of action for commercial misappropriation, and a statutory remedy for commercial misappropriation under the California Civil Code §3344.'[94] To state a common law cause of action for misappropriation, a plaintiff must plead sufficient facts to establish '(1) the defendant's use of the plaintiff's identity; (2) the appropriation of plaintiff's name or likeness to defendant's advantage, commercially or otherwise; (3) lack of consent; and (4) resulting injury'.[95] To state a statutory cause of action under §3344, a plaintiff must plead all the elements of the common law action and must also prove (5) 'a knowing use by the defendant' and (6) 'a direct connection between the alleged use and

the commercial purpose'.[96] This class action lawsuit could potentially approach 100 million people if they all agree to join (Segall, 2013). Facebook has offered to settle the lawsuit by making changes to its service terms to more clearly explain how 'Sponsored Stories' works.[97] Facebook also agreed to pay $20 million into a settlement fund.[98]

What is Facebook's 'Friend Finder'?[99] The 'Friend Finder' is a feature of Facebook, allowing users to integrate their other Internet accounts (e.g. Skype, Email, iCloud, Aim, Yahoo etc.) to invite those contacts to join Facebook or search for potential contacts and suggest them as 'friends'.[100] You can also search for 'friends' using their full names or email addresses.[101] Facebook states the option of allowing yourself as the user, once you upload another account of contacts to Facebook, it will not store any further information once you choose to delete it. However, one user detailed her experience of allowing Facebook access to her private information of her contact list was a bad idea.[102] The 'Friend Finder' service still notified her of potential 'friends' she may have interest in adding, even after her deletion of her outside accounts.[103]

As always, Facebook is business thinking on how to be more profitable at the users' expense of privacy. Just recently, Facebook has released a beta version of 'Graph Search' (Stocky & Rasmussen, 2013). Graph Search seems to be a more personalized to your specific searches, instead of how typical searches on 'Google' would populate the popular links. Search results are based on both the content of the user and their friends' profiles and the relationships between the user and their friends. Results are based on the friends and interests expressed on Facebook, and also shaped by users' privacy settings.[104] In addition to being restricted from seeing some content, users may be able to view relevant content made publicly available by users that are not listed as friends.[105] This is a great way to keep people using the Facebook network longer for purposes other than typical Facebook browsing of about seven hours a month.[106] Some benefits Facebook can receive for this 'Graph Search' would be more time users spend on the website, allowing more advertisers and marketers to spend more with Facebook in order to reach out for those potential users.

Another innovation in the works still waiting official release from Facebook is similar to a house arrest ankle bracelet, better known as a 'Location Tracker' app designed for smartphones[107] that can track your location.[108] This rumored app would allow your location at all times to be up-to-date, and at any time displayed to other 'friends'.[109] Essentially this is strikingly similar to a Global Positioning System (GPS), but a typical GPS does not turn on by itself when the users intention is to keep it off. 'The app, scheduled for release by mid-March (2013), is *designed to help users find nearby friends and would run even when the program isn't open on a handset*.'[110]

Talk about privacy infringement this app would take the cake for this. Do you see the pattern yet? All these features seem appealing to the advancement of society at first, but contrary to that appeal, it may hold consequences down the road. The privacy infringements that society currently allows social media sites to get away with, will be the ruination of the world by causing serious consequences that can haunt us in the future when applying to schools, job positions, maintaining relationships, and civil or criminal trials.

7. Electronic innovation 'GPS' under the Fourth Amendment

Mobile devices today have changed the way people conduct their professional and personal lives. Most smartphones today have the capability to offer GPS or location tracking capabilities. This becomes a major constitutional issue when a website such as Facebook, proposes a location finder application that will unveil your location to Facebook and other users of the Facebook network.

A recent decision decided by the Supreme Court in *United States* v. *Jones*[111], involved a global positioning system[112] ('GPS') placed on a suspect's car by the FBI for purposes of tracking the vehicle's movements. The Court held that the installation of a GPS device on the vehicle constituted a 'search' in violation of Jones' Fourth Amendment rights.[113]

In 2004, the FBI and Metropolitan Police Department suspected Antoine Jones, the owner of a nightclub in the District of Columbia, of trafficking narcotics.[114] Officers employed various investigative techniques, which included: visual surveillance of the nightclub; installation of a camera focused on the front door of the club; a pen register; and wiretap covering Jones' cellular phone.[115] Based on information from these sources, the Government applied to the United States District Court for the District of Columbia for a warrant authorizing the use of a GPS device on the Jeep registered to Jones' wife.[116]

A warrant issued, authorizing installation of the device in the District of Columbia and within 10 days.[117] On the 11th day, and not in the District of Columbia but in Maryland, agents installed the GPS under the Jeep while it was parked in a public parking lot.[118] Over the next 28 days, the device tracked the vehicle's movements, and once the agents had to replace the device's battery when the vehicle was parked in a different public lot in Maryland.[119] By using multiple satellites signals, the device established the vehicle's location within 50–100 feet, and communicated that location by cellular phone to a Government computer.[120] It relayed more than 2000 pages of data over the 4-week period.[121] This was decided in favor of Jones' due to the lengthy monitoring considered a 'search' that occurred by the Government.[122]

Later cases have applied the analysis of Justice Harlan's concurrence in *Katz*, which said that a violation occurs when government officers violate a person's 'reasonable expectation of privacy'.[123] The Government argued the Harlan standard showed that no search occurred, since Jones did not have a 'reasonable expectation of privacy' in the area of the Jeep underbody and in the locations of the Jeep on the public roads, which were visible to all.[124] 'A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.'[125] But we need not address the Government's contentions, because Jones' Fourth Amendment rights do not rise or fall with the Katz formulation.[126] The Fourth Amendment was understood to protect 'persons, houses, papers, and effects it enumerates'.[127]

'The *Jones* concurrence, explained the transmission of electronic signals without trespass would remain subject to *Katz* analysis.'[128] Most importantly, cell phones and other wireless devices are now permitting wireless carriers to track and record the location of users.[129]

In the age before computers, the greatest protections of privacy were neither constitutional nor statutory, but practical.[130] Traditional surveillance was difficult and costly and, therefore, rarely taken.[131] This case would have required a large team of agents, multiple vehicles, and perhaps aerial assistance.[132] An unusual importance might have justified such an expenditure of law enforcement resources.[133] Devices like the one used in the present case, however, make long-term monitoring relatively easy and cheap.[134] 'In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative.'[135] 'A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way.'[136]

8. The turn against social media users

There have been persuasive court decisions, dealing with Facebook users' right to privacy of their information of what is placed on social networking sites. In many instances, when

the courts decide to invade a Facebook user's privacy of their account, the decision is usually made regarding discovery during preliminary trial hearings.

A New York State trial court in *Romano* v. *Steelcase Inc.*, 30 Misc. 3d 426 (N.Y. Sup. Ct. 2010), ruled against a Facebook user's right to privacy of their profile for reasons of discovery.[137] The case involved a controversy over the physical condition of the plaintiff, who claims to have sustained permanent injuries as a result, has affected her enjoyment of life.[138] The defense moved to admit material evidence that may be relevant to both the issue of damages and the extent of the plaintiff's injury, including a plaintiff's claim for loss of enjoyment of life.[139] The Romano court relied on plain language of the New York Statute CPLR §3101,[140] which gave the court a broad power of discretion in the supervision of discovery by determining what is 'material and necessary'.[141] The court defined 'necessary' as interpreted as meaning 'needful' and not indispensable'.[142] The 'material and necessary' standard is to be interpreted liberally, requiring disclosure of 'any facts bearing on the controversy which will assist preparation for trial by sharpening the issues and reducing delay and prolixity'.[143] The test is one of 'usefulness and reason'.[144] Discovery requests should be taken on a case-by-case basis, while 'upholding the public policy of favoring in open disclosure to keep fairness intact'.[145] 'If the information sought is sufficiently related to the issues in litigation so as to make the effort to obtain it in preparation for reasonable trial, then discovery should be permitted.'[146]

'The court stated that the Plaintiff's entries of her Facebook account would not be a violation of her right to privacy, and regardless of any concerns are outweighed by the defendants need for information.'[147] Further analogizing by the court states that a user's reasonable expectation of privacy in Internet postings or emails that have reached their recipients, does not afford those individuals any expectation of privacy.[148] 'Thus, when the Plaintiff created her Facebook and MySpace accounts, she consented to the fact that her personal information would be shared with others, notwithstanding her privacy settings.'[149] Since the Plaintiff was aware that any of her information might become publicly available, she cannot now claim that she had a reasonable expectation of privacy.[150]

As recently set forth by commentators regarding privacy and social networking sites, given the millions of users, '[i]n this environment, privacy is no longer grounded in reasonable expectations, but rather in some theoretical protocol better known as wishful thinking'. 'No person would have reasonable expectation of privacy where person took affirmative act of posting own writing on MySpace, making it available to anyone with a computer and opening it up to public eye' (Fleming & Herlihy, 2009).[151] The Romano court ruled in favor of Steelcase Inc., affording no protection of privacy to postings made to Facebook or any other social media site, since the purposes of such sites is to network by information shared by you or received.[152]

Another court decision to agree with the Romano court is *McMillen* v. *Hummingbird Speedway, Inc.*, 2010 Pa. Dist. & Cnty. Dec. LEXIS 270, which acknowledged everything posted to any social media site has no expectation of privacy and is deemed discoverable.[153]

In *Warshak* v. *United States*, 631 F.3d 266 (6th. Cir. 2010), the court held that a user does have a Fourth amendment right to privacy in emails sent, even when sent through a third party Internet Service Provider.[154] Most people do not hold an expectation of privacy of emails they address to another and send through their Internet Service Provider. It is very similar to sending an addressed envelope through the United States Post Office and not expecting the mailman to look at the address listed on the letter. Very similar to *Smith* v. *Maryland*, where the Court held that pen register to record numbers dialed from Smiths home telephone did not constitute a search, because it did not reveal who was on the other line or when it was completed.[155] 'There is no constitutionally protected

reasonable expectation of privacy in the numbers dialed into a telephone system.'[156] 'A person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.'[157] This has been coined as a waiver of reasonable expectation of privacy or implied consent to search.[158]

In *O'Leary* v. *Florida*, No. 1D12-0975, 2013 Fla. App. LEXIS 4221, at 1 (Fla. Dist. Ct. App. March 18, 2013), the court has decided that a Facebook page can be considered a means of 'sending' threats to others.[159] The defendant had posted language that was considered to be threatening on Facebook about a relative and same-sex partner.[160] The defense relied on Florida Statute Section 836.10, Florida Statues (2012), provides:

> Any person who writes or composes and also sends or procures the sending of any letter, inscribed communication, or electronic communication, whether such letter or communication be signed or anonymous, to any person, [6] containing a threat to kill or to do bodily injury to the person to whom such letter or communication is sent, or a threat to kill or do bodily injury to any member of the family of the person to whom such letter or communication is sent commits a felony of the second degree.[161]

The defense argued 'sending' under §836.10, did not apply to a Facebook post.[162] The trial court felt differently in two ways. First, the post was public and made viewable by any public user, and second the posting was an electronic communication sent to the recipient, which threatened to kill or do serious bodily harm to a member of the recipient's family.[163] The Florida appeals court affirmed the trial court's reasoning.[164]

A New York City officers' MySpace and Facebook page were used at trial for purposes of impeachment, in a trial accusing the arrestee for carrying a loaded weapon (Dwyer, 2009). The defense council brought up the police officer's MySpace page during trial, pointing out that it was set to a 'devious' mood setting after he watched the 2001 movie "Training Day".[165] The officer then posted on his Facebook page 'Vaughan is watching "Training Day" to brush up on proper police procedure.'[166] This has led to social media as another avenue for parties at trial for evidence of discoverability, taking into account credibility and genuine statements.

Internationally, an Australian court ruled that notice can be satisfied for default judgments by Facebook communication.[167] In the USA, no decision has been found from any court in allowing service by Facebook or Twitter.[168] There are a few concerns such as: a person registering for a social networking profile may not be who he or she claims to be; and infrequent users of social media accounts may not receive actual notice.[169] Service by email has been recognized in New York, Australia, and the UK.[170]

9. Conclusion

As time goes on and the Internet evolves daily, we need to protect our privacy with greater care. The less care we use, the less rights we shall have, and it is a proven fact. There is a growing trend by the courts to rely on old case law and statutes not created for purposes of the endless growing Internet. There is not one solution that may best fix this problem, but awareness of your privacy rights while online using social media services or email is a start. You can show a subjective expectation in privacy of your online networking, or emailing by using encryptions, or passwords. There are some protective measures that can be suggested here to protect our privacy on social media sites.

First by allowing servers to track our locations, we can accept the use of anonymous servers that will allow blurring our location information (Voulodimos & Charalampos,

2009). As we use highly accurate location information devices, we consent to more of a generic location to be broadcasted to others rather than our home address or exact location, such as nearby cities, or landmarks. The choice of privacy is left in you as the user of the technology to choose what you broadcast, or allow.

Second, we live in a free market society where no one forces us to buy luxury items such as smartphones. The choice of a smartphone, enables us to connect to the Internet and if we choose to subscribe to social media networks that can result in our location being infringed on or diminished privacy rights. The 'posting' to Facebook of our thoughts, ideas, pictures, videos, or criticism, becomes bound to the terms of service or agreement, the privacy settings, and the intent to the public of what they can view, comment, or share without limitations.

Other potential remedies should come from legislatures. Collectively our greatest voice is the people and what they believe is private and should be protected. Since legislatures are directly connected with their constituents, they remain in the best position to discuss, debate, and create laws that can protect our privacy. A panel made up of local and federal governments may convene people with expertise with online privacy to recommend new laws and statutes to protect the American people's rights.

The issue of Internet privacy dealing with social media networks and emails is a gray area at best. As time passes, there are more debates and cases that involve some sort of problem related to social media. There have been no definitive laws that have been clear and ambiguous on this topic. The Computer age is here and we need to pressure Congress and state legislatures to create an understanding that is universally acceptable. We need to think about public policy going forward and design a system that will be informative and fair for all, especially if we continue on the path we are currently on. Would not it be pretty to think so?

Notes

1. U.S. CONST. amend. IV.
2. *Katz* v. *United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). The '*Katz* test' refers to the two-pronged test proposed in Justice Harlan's *Katz* concurrence and later adopted in full by the Court.
3. What is a tablet PC?, *wiseGEEK*. Retrieved from http://www.wisegeek.org/what-is-a-tablet-pc.html (last accessed 15 March 2013). A tablet personal computer is a cross between a laptop or notebook computer and a personal digital assistant (PDA). It's essentially a flat-panel portable computer. The user either taps on the screen with his or her finger or with a stylus, or he or she uses a stylus to write on the screen. A tablet PC can wirelessly connect to the Internet and other computers. The term 'tablet PC' originally referred to a specific brand or tablets that were compatible with certain operating systems, but any tablet-sized computer has come to be referred to in some instances as a tablet PC. The main feature of a tablet computer is portability.
4. Liane Cassavoy, What is a smartphone?, *About.com*. Retrieved from http://cellphones.about.com/od/glossary/g/smart_defined.htm (last accessed 15 March 2013). A smartphone is a device that lets you make telephone calls, but also adds features that you might find on a personal digital assistant or a computer. A smartphone also offers the ability to send and receive email and edit Office documents, for example.
5. What is a PDA personal digital assistant?, *wiseGEEK*. Retrieved from http://www.wisegeek.org/what-is-a-pda-personal-digital-assistant.htm (last accessed 15 March 2013). A PDA is a handheld device designed to help people organize their lives while on the move. While the original PDAs were somewhat limited to storing addresses, phone numbers, calendar appointments, and task lists, modern PDAs often work as a cell phone and fax, provide Internet connectivity, and much more. There are many different types, but almost all models can connect to a computer to sync information and access other optional features. Nearly all PDAs include

standard organizer features, such as an appointment calendar and task list. Some models come with a broader suite of software programs already installed, while others offer optional additional programs, often for an additional price.

6. Walt Howe, An anecdotal history of the people and communities that brought about the Internet and the Web. A brief history of the Internet (13 September 2012), *WaltHowe.com*. Retrieved from http://walthowe.com/navnet/history.html.
7. Kipp Bodnar, The ultimate glossary: 120 social media marketing terms explained (30 December 2011), *HubSpot*. Retrieved from http://blog.hubspot.com/blog/tabid/6307/bid/6126/The-Ultimate-Glossary-120-Social-Media-Marketing-Terms-Explained.aspx.
8. Help, *Facebook*. Retrieved from https://www.facebook.com/help/219375581424410/ (last accessed 15 March 2013). A 'daily active user' is considered to be active when they view or engage with your application or your application's content.
9. Facebook Privacy Policy, *Facebook*. Retrieved from https://www.facebook.com/full_data_use_policy (last accessed 15 March 2013).
10. Id.
11. Encyclopedia, Terms of service definition from PC magazine encyclopedia, *PCMag.com*. Retrieved from http://www.pcmag.com/encyclopedia/term/62682/terms-of-service (last accessed 15 March 2013).
12. Sarah Perez, How to delete Facebook applications (and why you should), *ReadWriteWeb.com*. Retrieved from http://www.readwriteweb.com/archives/how_to_deletefacebookapplications_and_why _you_ should.php (last accessed 15 March 2013).
13. The previous policy was longer than the United States Constitution, which is 4543 words without any of its amendments.
14. Mark Zuckerberg, Making control simple (26 May 2010), *The Facebook Blog*. Retrieved from https://blog.facebook.com/blog.php?post=391922327130.
15. Facebook Privacy Policy, *Facebook*. Retrieved from http://www.facebook.com/about/privacy/ (last accessed 15 March 2013).
16. Id.
17. Id.
18. Christian Fuchs, What has changed and what do these changes mean? (14 December 2012), *Information – Society – Technology & Media*. Retrieved from http://fuchs.uti.at/841/.
19. Id.
20. Legal Terms, *Facebook*. Retrieved from http://www.facebook.com/legal/terms (last accessed 15 March 2013).
21. Id.
22. Id.
23. Id.
24. Id.
25. Id.
26. Id.
27. Facebook Privacy Policy, *Facebook*. Retrieved from https://www.facebook.com/full_data_use_policy (last accessed 15 March 2013).
28. Id.
29. Terms of Use, *Instagram*. Retrieved from http://instagram.com/about/legal/terms/ (last accessed 15 March 2013).
30. Id.
31. Id.
32. Id.
33. Paul Gil, What exactly is 'Twitter'? What is 'tweeting'?, *About.com*. Retrieved from http://netforbeginners.about.com/od/internet101/f/What-Exactly-Is-Twitter.htm (last accessed 15 March 2013).
34. Id.
35. Id.
36. Flipping the bird, *Urban Dictionary*. Retrieved from http://onlineslangdictionary.com/meaning-definition-of/flip-the-bird (last accessed 15 March 2013).
37. Katz, *supra* note 2, at p. 347.
38. Id. at p. 348.
39. Id.

40. Id. at p. 351.
41. Id. at p. 363.
42. Id. at p. 361.
43. Katz, *supra* note 2, at p. 361.
44. Id. at p. 351.
45. Id.
46. Id.
47. Id. at p. 361.
48. Id. (Harlan, J., concurring) (emphasis added).
49. *Smith* v. *Maryland*, 442 U.S. 735, 735 (1979) (majority opinion).
50. Id. at p. 740.
51. *United States* v. *White*, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting). *See generally* Leary (2011).
52. Id. at pp. 745–747 (majority opinion).
53. Id. at p. 747.
54. Id. at p. 752.
55. Id. at pp. 784–785 (Harlan, J., dissenting).
56. White, *supra* note 63, at p. 788 n.24 (Harlan, J., dissenting).
57. Id. at p. 786.
58. Id. at p. 786 (Harlan, J., dissenting).
59. Smith, *supra* note 61, at p. 750 (Marshall, J., dissenting).
60. Smith, *supra* note 61, at p. 751 (Blackmun, J., dissenting).
61. Id. at p. 737.
62. Id.
63. Id. at p. 741 n.5.
64. Id. at p. 741 n.5.
65. *Black's Law Dictionary* 519 (4th ed. 1996). The term 'normative' means '[e]stablishing or conforming to a norm or standard'.
66. E.g. *Bond* v. *United States*, 529 U.S. 338 (2000) and *California* v. *Ciraolo*, 476 U.S. 207 (1986). See generally Leary, *supra* note 63, 1059–1060.
67. *Minnesota* v. *Carter*, 525 U.S. 83, 97 (1998) (Scalia, J., concurring). See generally Leary, *supra id*.
68. US Department of Justice, Electronic Communications Privacy Act of 1986, 18 U.S.C. §2510–22 (21 March 2012), *Justice Information Sharing*. Retrieved from http://www.it.ojp.gov/default.aspx?area=privacy&page=1285.
69. Id.
70. Id.
71. Id.
72. Id.
73. Id.
74. Id.
75. Id.
76. Id. 'Pen register is a device that captures the dialed numbers and related information to which outgoing calls or communications are made by the subject.'
77. Id. Trap and trace is a device that captures the numbers and related information from which incoming calls and communications coming to the subject have originated.
78. Id.
79. Id.
80. *Lane* v. *Facebook, Inc.*, 696 F.3d 811, 816 (Cal. Ct. App. 2012).
81. Id. at p. 811.
82. Id.
83. Lane, *supra* note 96, at p. 816.
84. Id.
85. Id. at p. 827.
86. Id.
87. Help, *Facebook*. Retrieved from https://www.facebook.com/help/162317430499238/ (last accessed 15 March 2013). Sponsored stories are messages coming from friends about them

engaging with a Page, app or event that a business, organization or individual has paid to highlight so there's a better chance people see them.

88. Brittany Darwell, Understanding the difference between Facebook Sponsored Stories, page post ads, promoted posts and marketplace ads (11 January 2013), *InsideFacebook*. Retrieved from http://www.insidefacebook.com/2013/01/11/understanding-the-difference-between-facebook-sponsored-stories-page-post-ads-promoted-posts-and-marketplace-ads/.
89. Id.
90. Laurie Segall, Facebook could pay users in class-action Sponsored Stories settlement (28 January 2013), *CNN Money*. Retrieved from http://money.cnn.com/2013/01/28/technology/social/facebook-class-action/index.html.
91. *Fraley* v. *Facebook, Inc.* Retrieved from http://www.fraleyfacebooksettlement.com/ (last accessed 15 March 2013).
92. *Fraley* v. *Facebook, Inc.*, 830 F. Supp. 2d 785, 792 (N.D. Cal. 2011).
93. Id. at pp. 796–797.
94. Id. at p. 803.
95. Id.
96. Id.
97. Id.
98. Id.
99. Find Friends, *Facebook*. Retrieved from https://www.facebook.com/find-friends (last accessed 15 March 2013). Import contacts from your account and store them on Facebook's servers where they may be used to help others search for or connect with people or to generate suggestions for you or others. Contact info from your contact list and message folders may be imported. Professional contacts may be imported but you should send invites to personal contacts only. Please send invites only to friends who will be glad to get them. You can always manage your imported contacts or remove them completely.
100. *Cohen* v. *Facebook, Inc.*, 798 F. Supp. 2d 1090, 1092 (N.D. Cal. 2011).
101. Wingrider, Krystle, Spyagent, Jordan, et al., How to use the Facebook Friend Finder Tool, *wikiHow*. Retrieved from http://www.wikihow.com/Use-the-Facebook-Friend-Finder-Tool (last visited 15 March 2015).
102. Kenya, Facebook Friend Finder: What you may not know your data (22 June 2009), *gdgtgrl*. Retrieved from http://gdgtgrl.net/2009/06/22/facebook-friend-finder-what-you-may-not-know-about-your-data/. After deleting my stored contact information on Facebook, the service seems to be on overdrive recommending friends to me that are from my address book (three new ones today). Apparently, this information was not deleted. It's best not to let Facebook have access at all.
103. Id.
104. How privacy works with graph search, *Facebook*. Retrieved from https://www.facebook.com/about/graphsearch/privacy (last accessed 15 March 2013).
105. Id.
106. Mary Schwager, Facebook addicted? How much time do people really spend on Facebook? (17 February 2010), *Examiner.com*. Retreived from http://www.examiner.com/article/facebook-addicted-how-much-time-do-people-really-spend-on-facebook.
107. Liane Cassavoy, What is a smartphone?, *About.com*. Retrieved from http://cellphones.about.com/od/glossary/g/smart_defined.htm (last visited 15 March 2013).
108. Jared Newman, Friend finder or location tracker? Facebook's trust problem, visualized. (5 February 2013), *Time Tech*. Retrieved from http://techland.time.com/2013/02/05/friend-finder-or-location-tracker-facebooks-trust-problem-visualized/.
109. Id.
110. Id.
111. *United States* v. *Jones*, 132 U.S. 945, 949 (2012).
112. Margaret Rouse, Global Positioning System (GPS) (May 2007), *SearchMobileComputing*. Retrieved from http://searchmobilecomputing.techtarget.com/definition/Global-Positioning-System. The GPS is a 'constellation' of 24 well-spaced satellites that orbit the Earth and make it possible for people with ground receivers to pinpoint their geographic location. The location accuracy is anywhere from 100 to 10 meters for most equipment. Accuracy can be pinpointed to within one (1) meter with special military-approved equipment. GPS equipment

is widely used in science and has now become sufficiently low-cost so that almost anyone can own a GPS receiver. The GPS is owned and operated by the US Department of Defense but is available for general use around the world. Briefly, here's how it works: 21 GPS satellites and three spare satellites are in orbit at 10,600 miles above the Earth. The satellites are spaced so that from any point on Earth, four satellites will be above the horizon. Each satellite contains a computer, an atomic clock, and a radio. With an understanding of its own orbit and the clock, it continually broadcasts its changing position and time. (Once a day, each satellite checks its own sense of time and position with a ground station and makes any minor correction.) On the ground, any GPS receiver contains a computer that 'triangulates' its own position by getting bearings from three of the four satellites. The result is provided in the form of a geographic position – longitude and latitude – to, for most receivers, within 100 meters. If the receiver is also equipped with a display screen that shows a map, the position can be shown on the map. If a fourth satellite can be received, the receiver/computer can figure out the altitude as well as the geographic position. If you are moving, your receiver may also be able to calculate your speed and direction of travel and give you estimated times of arrival to specified destinations. The GPS is being used in science to provide data that has never been available before in the quantity and degree of accuracy that the GPS makes possible. Scientists are using the GPS to measure the movement of the arctic ice sheets, the Earth's tectonic plates, and volcanic activity. GPS receivers are becoming consumer products. In addition to their outdoor use (hiking, cross-country skiing, ballooning, flying, and sailing), receivers can be used in cars to relate the driver's location with traffic and weather information.

113. Jones, *supra* note 130, at p. 949.
114. Id. at p. 948.
115. Id.
116. Id.
117. Id.
118. Id. at p. 948.
119. Jones, *supra* note 130, at p. 948.
120. Id.
121. Id.
122. Id. at p. 965.
123. Id. at p. 948.
124. Id.
125. Jones, *supra* note 130, at p. 948.
126. Id. at p. 951.
127. Id.
128. Id. at p. 955.
129. CTIA Consumer Info, 50 Wireless Quick Facts, http://www.ctia.org/consumer-info/index.cfni/AID/10323 (last visited 15 March 2013). As of June 2011, it has been reported, there were more than 322 million wireless devices in use in the USA.
130. Jones, *supra* note 130, at p. 963 (Alito, J., concurrence).
131. Id.
132. Id.
133. Id. at pp. 963–964.
134. Id. at p. 964.
135. Id.
136. Jones, *supra* note 130, at p. 964.
137. *Romano* v. *Steelcase Inc.*, 30 Misc. 3d 426 (N.Y. Sup. Ct. 2010).
138. Id. at p. 427.
139. Id. at p. 428.
140. NY §3101 (2013).
141. Romano, *supra* note 156, at p. 427.
142. Id.
143. Id.
144. Id.
145. Id. at p. 428. 346 7960.
146. Id.
147. Romano, *supra* note 156, at p. 433.

148. Id.
149. Id. at p. 434.
150. Id.
151. *Dexter* v. *Dexter*, No. 2006-P-0051, 2007 Ohio 2568, 2007 Ohio App LEXIS 2388 (Ct App, 11th Dist, Portage County 2007).
152. Romano, *supra* note 156, at p. 434.
153. *McMillen* v. *Hummingbird Speedway, Inc.*, Dec. LEXIS 270 (Pa. Cnty. Ct. 2010).
154. *Warshak* v. *United States*, 631 F. 3d 266, 282 (6th Cir. 2010).
155. Smith, *supra* note 61, at pp. 745–746.
156. *Smith* v. *Maryland*, 283 Md. 156, 173 (Md. 1978), *aff'd*, 442 U.S. 735 (1979).
157. Smith, *supra* note 61, at pp. 743–744.
158. Kerr (2009). Explaining that the 'third-party doctrine' precludes an individual from claiming Fourth Amendment protection for information that was voluntarily revealed.
159. *O'Leary* v. *Florida*, No. 1D12-0975, 2013 Fla. App. LEXIS 4221, at 1 (Fla. Dist. Ct. App. March 18, 2013).
160. Id.
161. FL §836.10 (2012). Retrieved from http://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute& Search_String=&URL=0800-0899/0836/Sections/0836.10.html (last accessed 15 March 2013).
162. O'Leary, *supra* note 178, at p. 3.
163. Id. at p. 4.
164. Id.
165. Id.
166. Id.
167. Lisa McManus, Service of process through Facebook (10 March 2011), *LexisNexis Communities*. Retrieved from http://www.lexisnexis.com/community/international-foreignlaw/blogs/internationalandforeignlawblog/archive/2011/03/10/service-of-process-through-facebook.aspx.
168. Id.
169. Id.
170. Id.

References

Bilton, N. (2010, May 12). Price of Facebook privacy? Start clicking. *New York Times*. Retrieved from http://www.nytimes.com/2010/05/13/technology/personaltech/13basics.html?r=1

Campbell, A. (2011, March 7). What the heck is an 'app'? *Small Business Trends*. Retrieved from http://smallbiztrends.com/2011/03/what-is-an-app.html

Cranor, L. F. (2009, March 11). A guide to Facebook's privacy options. *New York Times*, p. R5. Retrieved from http://online.wsj.com/article/SB10001424127887324880504578300312528424302. html?mod=e2fb

Culter, K.-M. (2012, April 9). From 0 to $1 billion in two years: Instagram's rose-tinted ride to glory. *TechCrunch*. Retrieved from http://techcrunch.com/2012/04/09/instagram-story-facebook-acquisition/

Dwyer, J. (2009, March 11). The officer who posted too much on MySpace. *New York Times*, p. A24. Retrieved from http://www.nytimes.com/2009/03/11/nyregion/11about.html?_r=0

Fleming, D. L., & Herlihy, J. M. (2009). What happens when the college rumor mill goes online? Privacy, defamation and online social networking sites. *Boston Bar Journal*, *53*, 16.

Frommer, D. (2010, November 1). Here's how to use Instagram. *Business Insider*. Retrieved from http://www.businessinsider.com/instagram-2010-11

Hancock, C. (2009). Warrants for wearing a wire: Fourth Amendment privacy and Justice Harlan's dissent in *United States* v. *White*. *Mississippi Law Journal*, *79*, 35, at 76.

Hernandez, B. A. (2012, December 18). 15 Celebrities outraged by Instagram's Privacy Policy. *Mashable*. Retrieved from http://mashable.com/2012/12/18/celebrity-outrage-instagram-terms-of-service/

Kerr, O. S. (2009). The case for the third-party doctrine. *Michigan Law Review, 107*, 561–601.

Leary, M. G. (2011). Reasonable expectations of privacy for youth in a digital age. *Mississippi Law Journal*, *80*, 1033–1092.

Pepitone, J. (2012, December 18). Instagram can now sell your photos for ads. *CNNMoney*. Retrieved from http://money.cnn.com/2012/12/18/technology/social/instagram-sell-photos/index.html

Purewal, S. J. (2011, June 8). Why Facebook's Facial Recognition is creepy. *PCWorld*. Retrieved from http://gigaom.com/2011/11/14/court-makes-it-official-you-have-no-privacy-online/

Segall, L. (2013, January 28). Facebook could pay users in class-action Sponsored Stories settlement. *CNNMoney*. Retrieved from http://money.cnn.com/2013/01/28/technology/social/facebook-class-action/index.html

Semitsu, J. P. (2011). Social networking and the law: Article: From Facebook to mug shot: How the death of social networking privacy rights revolutionized online government surveillance. *Pace Law Review*, *31*, 291–381.

Smith, K. (2009, September 28). The 12 best social networking apps. *Business insider*. Retrieved from http://www.businessinsider.com/best-social-media-apps-in-the-world-2012-9?op=1

Stocky, T., & Rasmussen, L. (2013, January 15). Introducing graph search beta. *Newsroom*. Retrieved from http://newsroom.fb.com/News/562/Introducing-Graph-Search-Beta

Voulodimos, A. S., & Patrikakis, C. Z. (2009, December). Quantifying privacy in terms of entropy for context aware services. *Identity in the Information Society Journal* (special issue), *2*(2). Identity Management in Grid and SOA.