Facebook and Online Privacy Law

Craig Tierney

Butler University

JR 414: Mass Communication Law

Dr. Whitmore

December 14, 2015

Facebook and Online Privacy Law

It is free to create social media accounts, but the world of profiles, "likes," "reposts," and "walls" is a world of business. Like any other business, an exchanging of goods is taking place. Yet, if social media users are not paying for the accounts they create in these networks, then where is the money in social media? The money is in data - more specifically, the personal data of those who create and maintain social media accounts. [1]

According to Robert E. Lemons, Facebook is one of the biggest offenders when it comes to selling details about its users to advertisers and other third parties. [2] This is because the social media platform begun by Mark Zuckerberg is one of the largest (and in 2011, one of the fastest-growing) social media platforms around, with 40 percent of the U.S. population possessing accounts as of four years ago.[3] With personal data from this many people (not including the millions who have joined in the last few years), it is no wonder that Facebook is turning a profit. In light of this large benefit to a company offering a "free" service, Facebook users should be asking is what "free" actually means to them. What information does Facebook sell, and to whom? What personal data could they get in the future? And what do users agree to when they sign up? In short, what rights do users have when it comes to Facebook and privacy?

Social media is one of the newer technologies that has become so popular so fast that the law still needs to catch up. There are minimal laws in effect to govern this new frontier of privacy and there are still many questions to be answered concerning how much responsibility lays with those who create accounts and the social media companies themselves.[4] The Federal

---

[1] See Michael J. Kasdan, *Is Facebook Killing Privacy Softly? The Impact of Facebook's Default Privacy Settings on Online Privacy,* New York University Intellectual Property & Entertainment Law Ledger, 108 (2011)
[2] See Robert E. Lemons, *Protecting Our Digital Walls: Regulating the Privacy Policy Changes Made by Social Networking Websites,* A Journal of Law and Policy for the Information Society, 605 (2011)
[3] *Supra note 1*
[4] See Lemons, 607 (2011)

Trade Commission (FTC) has limited power over these platforms and Facebook, in particular, due to these unresolved questions.[5]

It is common knowledge that Facebook, like most other social media platforms, has a privacy policy that everyone who creates a profile must agree to before they can create a Facebook account. However, it is less commonly known how much that privacy policy has changed since Facebook's beginnings. [6] The platform began as a way for university students to connect with each other, featuring completely private pages and only names, profile pictures, and mutual "friends" being shared publicly (those who one was not "friends" with).[7] Over the years as Facebook expanded to include any and everyone with a valid email address, these privacy settings changed as well. The privacy settings became more complicated, but remained a customizable focus until 2007, when Facebook's "Beacon" came out.[8] Beacon was the first time that Facebook began to make users' names, birthdates, and geographic locations available to advertisers. There was an intense backlash and "Beacon" was shut down.[9]

In December of 2009, Facebook made a similar move that is now known unofficially as "The Great Betrayal."[10] With no notification to any Facebook users, the site made all general information from each and every account public – even information previously set as "private" by the user. The only option was to "opt out" or actively change a setting on one's account in order to make this data private once more.[11] Up until this point in time, the FTC had not solidified its role in governing the social side of cyber space. After "The Great Betrayal," the

---

[5] *Id*
[6] See Erica Jaeger, *Facebook Messenger: Eroding User Privacy in Order to Collect, Analyze, and Sell Your Personal Information,* The John Marshall Journal of Computer & Information Law, 398 (2014)
[7] *Id*
[8] See Lemons, 608 (2011)
[9] *Id*
[10] *Id*
[11] *Id*

FTC reviewed Facebook's own privacy policies and subsequently filed a lawsuit with no less than eight complaints that the company had violated its own privacy policies.[12] These complaints included that Facebook provided unnecessary user information to advertisers and applications that interacted with the website in addition to the fact that users had no notice or say in the changes in the privacy policy.[13] The FTC settled with Facebook after the company agreed to adhere to its own terms in the privacy policy while also maintaining better communication with the platform's users in regards to future changes to the privacy policy.[14]

A quick foray into the current privacy settings on Facebook show that every piece of information is set to "public", meaning anyone on Facebook and possibly those who search for a person on Google can see that person's profile. Each individual piece of information, application, and status have privacy settings of their own. One must change the privacy settings for each of these smaller pieces in order to ensure only "friends" can see Facebook activities. The presence of these customizable options appear to be helpful, but when default settings make everything "public" from the start, problems could arise.[15] Hackers and identity theft immediately spring to mind – these criminals can do a lot of damage with minimal information (e.g. name, hometown, birthdate, etc.).[16] In addition, page "likes" are public and can lead to others deducing facts about a person from their associations and endorsements of Facebook pages, even when that person may trust the default settings and believe these endorsements are private.[17] The default "public" settings have been psychologically tested and results have shown the majority of users

---

[12] See Claudia Bourne Farrell, *Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises,* Federal Trade Commission, 1 (2011) https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep
[13] *Id*
[14] *Id*
[15] See Kasdan, 113 (2011)
[16] *Id*
[17] See Lemons, 609 (2011)

automatically select (unknowingly) for their activity on Facebook to become "public."[18] When these kinds of issues arise from "public" settings, there is an apparent and unregulated privacy issue at hand.

Even today, the power has not shifted much more towards any federal regulation of social media platforms when it comes to user privacy.[19] This is an important issue because every day, millions of people log in to Facebook to post, share, and associate themselves with other people, ideas, and things. Their locations, likes, dislikes, and demographics are available online only to those who they connect with – or so they think. The goal of this paper is to answer the question: How much of a right to privacy should one have when they sign up for Facebook? Court cases involving this social media site will be examined and compared to the scholarly opinions of legal journalists in order to answer this question.

This paper argues that Facebook has a transparency issue when it comes to the site's privacy policy. Allegations of recommended privacy settings that actually leave most information public until changed are among the most common, in addition to: "reidentification,"[20] lack of differential privacy, and a loose definition of "general information" on Facebook.[21] Better governmental regulations need to be updated and tailored to define and protect the privacy of Facebook users (as well as users of other social media platforms). Social media and the Internet in general are relatively new phenomenons, so the law has yet to fully catch up. This results in grey areas of privacy that need to be resolved for the sake of 40 percent of Americans whose private data could be at risk every day they possess a Facebook account.

---

[18] *Id*
[19] See Farrell (2011)
[20] See Andrew Chin and Anne Klinefelter, *Social Networks and the Law: Differential Privacy as a Response to the Reidentification Threat: The Facebook Advertiser Case Study*, North Carolina Law Review Association, 160 (2012)
[21] *Id*

Part I of this paper will further delve into Facebook's past privacy policies and changes, including analyses of court cases having to do with these changes. Part II will look at what online privacy should mean, again looking at court cases in order to build the beginnings of a definition. Part III of this paper will suggest changes in the law and Facebook's operations that have already or need to happen as a result of court cases and current privacy policies.

Currently, Facebook provides simple tabs and a drop down menu full of privacy options – everything from deciding who can view a user's posts to what kind of advertisements the user wants to see. The privacy settings are easy to use, set up in a question and answer format. "Who can see your future posts?" asks one, followed by a "yes" or "no' answer with the option to edit. There is even a tab that allows users to edit what Facebook activities can be shown in ads on friends' homepages and what ads should be shown on their own profiles based on their input of interests. While this sounds like a perfect system, it has not always been this way. Even today there are large imperfections, such as the noticeable lack of settings concerning what third parties can access someone's Facebook profile and activity information.

A good place to begin analyzing Facebook's past issues with privacy is the case of *Cohen, et al. v Facebook* (2011). In this case, Robyn Cohen, a Facebook user (and others), attempted to sue the social media corporation for using his name and picture in advertisements for the website's "Friend Finder" service.[22] The ads used the plaintiffs' names and pictures, displaying them to other users alongside messages like "Robyn Cohen used Friend Finder. Try it now!"[23] Not only did Facebook display these users' full names and images, it highlighted their activities on the website by saying they utilized the "Friend Finder" feature.[24] Facebook was

[22] See *Robyn Cohen, et al. v Facebook, Inc.*, 798 F. Supp. 2d 1090, 18 (N. D. Cal., 2011)
[23] *Id*
[24] *Id*

clearly trying to encourage its members to use this feature by showing that others had done so, but it is questionable how much information they were willing to share of its members in order to achieve this goal – which is why Cohen and the others sought legal action. This case raised a good question: where did Facebook draw the lines for users' privacy?

This case was dismissed by the court due to the plaintiffs' failure to prove any monetary or personal harm as a result of the advertisements.[25] In this case and many others that will be discussed, Facebook did not necessarily cause financial or reputational harm to its members. Instead, it created distress due to the dissemination of personal information without notification or clear policies. It is much harder to prove harm due to discomfort in a court of law.

A similar case played out involving the Pandora music iPhone application in 2013.[26] Troy Yunker, who used the Pandora app on his iPhone, discovered that the company was sending data about its users to third party advertisers without depersonalizing it.[27] This means that instead of sending generic demographics in bulk (e.g. "Indianapolis listeners are typically male, aged 25, interested in fitness"), Pandora was sending advertisers specific details that could lead to the identification of individuals.[28] This kind of activity was expressly prohibited in Pandora's own privacy policy, but because Yunker and the other plaintiffs could not prove any harm, the case was dismissed.[29]

While Pandora could be commended for even including this kind of detail in their privacy report (unlike the rather broad language that Facebook used to use[30]), it should be worrying to people who use these phone applications and websites that this company was not held

---

[25] *Supra note 22*, 22
[26] See *Troy Yunker, et al., v Pandora Media Inc*., 2013 U.S. Dist. LEXIS 42691, 3 (2013)
[27] *Id*
[28] *Supra note 26*, 4
[29] *Supra note 26*, 49
[30] See previous cases

accountable by the court to make right on its own privacy policy. If the contract for use created by an online company cannot keep that company accountable in a court of law, then there is an issue with how the law handles the new technologies that are social websites and phone applications.

The case of *Fraley v Facebook* (2011) played out in much the same way. Angel Fraley and other Facebook members attempted to sue the company for using their names and images in advertisements of products and services they had "liked" on the website.[31] These advertisements (dubbed "sponsored stories" by Facebook[32]) encourage users to follow pages for various services and products by showing that their friends follow them. Fraley and the others argued that this was a privacy violation because not only did it use their names and pictures in the advertisements (as in Cohen's case), Facebook also publicly displayed the products and services that the users had chosen to follow.[33] The public display of this kind of activity to other Facebook users is made worse due to the messaging in the advertisements because it seems as if the users are endorsing or supporting the pages they have "liked."[34]

Once again, Facebook was able to get the charges dismissed; however, they had better reasoning this time. Included in the privacy policy (at that time in 2011), the company had included a statement saying users' general information (name, profile picture, and "likes") could be used for in-site advertising.[35] It appears Facebook had learned from earlier cases like *Cohen*, and decided to include clearer statements concerning what the website wanted to be able to use in its own advertisements. Fraley and the others were unable to show proof of financial or any

---

[31] See *Angel Fraley, et al. v Facebook, Inc.*, 830 F. Supp. 2d 785, 4 (N. D. Cal., 2011)
[32] *Id*
[33] *Supra note 26*, 5
[34] *Id*
[35] *Supra note 26*, 79

other harm, and the fact that they had agreed to the privacy statement, including the piece about Facebook advertisements, so the court decided they had no case.[36] Once again, the plaintiffs' peace of mind was held to not be of circumstance – Facebook had managed to bury this piece of policy in its often unread Terms of Use agreement. It is there, but (as all Facebook users know), it is not easy to find. Terms of Use agreements are commonly known to be long, vague, and almost impossible to entirely read unless one has a law degree and plenty of time on their hands.

A good case to demonstrate the vagueness of most contracts, and which was used as part of Fraley's case, is *Marder v Lopez* (2006). The movie *Flashdance* was inspired by the life story of Maureen Marder, an exotic dancer who had some signature moves for her personal brand.[37] Marder sold the rights to her story to Paramount Pictures for only $2,300 – if she had read the contract closely enough, she would have realized the vague language stated she would receive none of the profits from the movie or any connected products.[38] Subsequent to the movie's release, Jennifer Lopez made a music video linked to the film which featured the pop star performing some of Marder's dance moves (also seen in the film).[39]

When Marder attempted to get her cut of the profits from both the film and the popular music video, she was denied by Paramount which claimed that in her contract she had sold all of the rights to her story to the company. This meant Paramount stood to profit off of Lopez's video because she had paid them to use the rights.[40] Marder sought legal action against Lopez, Sony Music, and Paramount because she claimed her rights to her own story were being infringed upon and she deserved to be compensated.[41] The court decided, after looking over the contract,

---

[36] *Id*
[37] See *Maureen Marder v Jennifer Lopez, Sony Music Ent., and Paramount Pictures*, 450 F. 3dd 445, 2 (2006)
[38] *Supra note 32*, 9
[39] *Id*
[40] *Supra note 32*, 20
[41] *Id*

that Marder had legally sold her rights to the story so there was no case. However, the court noted that the contract was written in extremely broad language such that Marder could have no case at all against Paramount or the others because all arguments were encompassed in the broadness of the terms.[42]

Returning to the topic at hand, Facebook has avoided a fair number of privacy lawsuits in the past due to their own long and vague privacy policies. Marder's case explains in part how Cohen and Fraley lost their cases. Not only is there broad language to be dealt with, but also the legal recognition of feelings of insecurity caused by breached privacy online. Privacy violations online have historically only been recognized when the plaintiff suffers financial or other harm that creates physical evidence. In regards to Facebook and other social media platforms that use and store personal data, the law needs to adapt to ensure peace of mind for members of these websites.

In order to adapt in such a way, there needs to be a good idea of what online privacy law should entail. A logical place to begin forming this definition is with cases concerning the "Big Brother" side of Facebook and other social media platforms.

In June of 2015, Matthew Campbell sued Facebook for one such incidence.[43] Campbell and others alleged that Facebook was scanning messages that users could send to one another privately - as the website itself claimed. Their evidence: once they mentioned or shared a link from a sponsored page (without having "liked" the page previously), the page would get an increase in "likes" and the user who shared the content would be automatically added to its list of followers.[44] This meant, claimed the plaintiffs, that Facebook was scanning users' private

---

[42] *Id*
[43] See *Matthew Campbell, et al. v Facebook, Inc*., 77 F. Supp. 3d 836, 3 (2015)
[44] *Id*

messages and obtaining information from them. The plaintiffs sued for wiretapping among other actions.[45] While the court dismissed this wiretapping charge (claiming that the users had consented to letting the website scan their content in agreeing to the Terms of Use privacy policy)[46], Facebook was caught in California's Invasion of Privacy Act because the company had technically intercepted messages that users were led to believe were private.[47] This case is recent, so it shows movement in a positive direction for online privacy laws, but the fact that in 2015 Facebook was scanning supposedly private messages is disconcerting. Online privacy law needs to decide how much power social media websites should be able to have in order to protect the millions of people in the U.S. who use them.

A similar case made by Barbara Moskowitz and others regarding Facebook's dissemination of user information to third party advertisers for a profit.[48] The complaint against the website alleged that when users clicked on advertisements, Facebook would automatically send details of the page currently open to the advertiser in question.[49] The advertisers wanted to know what pages on Facebook gave them the most traffic for their advertisements – the only problem was that often time users were clicking on the advertisements from their own profile pages.[50] This meant the third party advertisers were receiving much of the personal information posted on the profiles of each member who clicked on advertisements.[51] There was no provision for this spread of information in Facebook's privacy policies, so the plaintiffs attempted to sue for Breach of Contract.[52] Once again, Facebook wanted the charges dismissed due to the failure

---

[45] *Id*
[46] *Supra note 38*, 18
[47] *Id*
[48] See *In re Facebook Privacy Litigation*, 791 F. Supp. 2d 705, 3 (2011)
[49] *Id*
[50] *Supra note 43*, 4
[51] *Id*
[52] *Id*

of the plaintiffs to prove financial or other harm as a result of advertisers receiving profile information.[53] The company succeeded and also avoided Breach of Contract for the same reasons.[54] The plaintiffs had also attempted a charge of wiretapping, but because Facebook was not actively sending profile information out (it was automatically sent out in specific cases where users were on their profile page when they click an advertisement) this was also dismissed.[55]

In short, Facebook members were able to show that the website was sending out private information to third parties (in exchange for money), but due to the lack of online privacy laws, the courts dismissed the case with nothing to give the plaintiffs security over their personal details. The results of this case make Facebook seem more than ever like "Big Brother."

A similar case was made against LinkedIn in *Low v LinkedIn Corp*. (2011). Kevin Low and other LinkedIn members complained that the social networking site was sending cookies (records of online activity) to third party advertisers without users' consent.[56] Just as in the previous case against Facebook, LinkedIn avoided the charges because the users could not prove harm.[57]

This case expands the horizon to show that Facebook is not the only social media site with these issues. It appears that most social websites and applications make money by selling users' personal information without consequence or regulation. If this is the case, another question for the law arises: How can Facebook (or any social media company for that matter) be used without fear of private information being dispersed with no legal actions to support its members against the loss of privacy?

---

[53] *Supra note 43*, 6
[54] *Supra note 43*, 30
[55] *Supra note 43*, 32
[56] See *Kevin Low, et al., v LinkedIn Corporation*, 2011 U.S. Dist. LEXIS 130840, 3 (2011)
[57] *Supra note 50*, 15

While Facebook appears to be the bad guy in most of these cases involving privacy, there are a few cases where the company actually tried to protect the privacy of its users. The issue is: they still win court cases easily due to the lack of online privacy laws.

One such case is *Young v Facebook* (2010). Karen Beth Young was an up-and-coming public figure for her work in cancer research. In an attempt to gain followers and "likes" on her public page, Young began sending out hundreds of friend requests to people she did not know in real life.[58] Facebook subsequently deactivated her account multiple times because they said she was invading the privacy of others by soliciting so many unprovoked "friend requests."[59] While this part of the situation sounds reasonable, the case becomes worrisome when one reads how much time and effort it took Young to receive an answer as to why her account had been deactivated.[60] A small notification informed her of the deactivation of her account, but many phone calls and even a visit to Facebook headquarters were required for her to learn the simple answer that Facebook believed she had been invading others' privacy.[61] Facebook once again got the charges against them dismissed,[62] but that actually is not the issue in this case. The problem made evident here is that the company did not have to explain itself, even in a court of law. The court did not require that Facebook provide a good defense, even for the fact that Young was not clearly and duly notified as to why her account was deactivated.[63] This kind of freedom for Facebook is unsettling. With all of the personal information it contains from the millions of users who trust it is secure, it should have to answer to those same users especially in a court of law.

---

[58] See *Karen Beth Young v Facebook, Inc.*, 2010 U.S. Dist. LEXIS 116530, 3 (2010)
[59] *Id*
[60] *Id*
[61] *Supra note 52*, 4
[62] *Supra note 52*, 18
[63] *Id*

However, this case shows that online privacy laws are still too outdated to provide social media members with any protection.

It is now obvious that the law has some catching up to do. New technologies like social media and the mobile applications they create and that are used by so many people worldwide are currently in a grey area of the U.S. courts and legal system. The country recognizes that every citizen has a right to privacy, but how can these older laws be made (and kept) current to stay level with the new forms of communication and socialization consistently being created? Now this research will attempt to answer that question.

One of these new areas is the development of Facebook applications. These are games, quizzes, and other activities developed by a third party and authorized by Facebook so that members of the social media site can link their profiles to the applications in order to share their scores and challenge their friends.[64] For these applications, just like members, Facebook has created various policies, including those that concern copyrights – such as in the case of *Miller v Facebook* (2010).[65] This case revolved around a Facebook game named "ChainRxn" which was published as an application on the website after another game called "Boomshine," a similar game with a different author.[66] Facebook's own policies prevent the company from infringing on the copyrights of the applications it publishes, yet this is exactly what it did in this case by publishing a game that was too similar to the first for it to be protected under Fair Use laws.[67]

For this reason, Miller, the creator of "Boomshine," sought legal action to hold Facebook accountable for its own policies and to protect his copyright.[68] Eventually, Facebook removed

---

[64] See Facebook Developers website https://developers.facebook.com/
[65] See *Daniel M. Miller v Facebook, Inc. and Yao Wei Yeo*, 95 U.S.P.Q. 2D (BNA) 1822, 2 (2010)
[66] *Id*
[67] *Supra note 63*, 4
[68] *Id*

"ChainRxn" from its site, but it only happened after Miller took the matter to court – not when Miller initially sent the company complaints about the copyright protection of "Boomshine."[69]

While this case concerned copyright law, the take-away is that as recently as 2010, Facebook was guilty of not paying attention to or honoring its own policies: policies meant to protect the people who used its website and phone application. As was previously demonstrated by the analysis of *Yunker v Pandora,*[70] it appears that some of the most famous social websites have had trouble sticking to their own policies. This means that the people who use these forms of social media need to police it themselves. The cases studied in this research should remind members of Facebook and other online platforms that while these services are free to use, they are still businesses. These websites and applications are all still competing and are out to make a profit – something that may be easy to forget when anyone in the world can connect without spending a cent. Presently, when it comes to a user's privacy, it is up to that individual to be aware of what personal information they share because these cases have shown that the legal system had not been updated yet. Without legal reform, members of social media need to police the organizations themselves, yet even this is problematic without the proper laws to back up the people. For these reasons, and for the fact that millions of Americans use Facebook and other social media[71], it is clear that the government should make online privacy law a priority.

This priority doubles with the rising number of mobile users as demonstrated by the *iPhone Application Litigation* (2012) case.[72] In this case, the plaintiffs attempted to sue Apple, Inc. due to company sharing personal details and geographic locations with the third parties who

---

[69] *Id*
[70] See pg. 6
[71] See Protalinski, Emil, *Facebook passes 1.44B monthly active users and 1.25B mobile users; 65% are now daily users*, VentureBeat.com (2015)
[72] See *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 10 (2012)

developed iPhone applications the plaintiffs were utilizing.[73] The dispersion of this information was not made plain to iPhone users in any method, so the plaintiffs had downloaded applications which received the information stored on the devices themselves, seemingly untouchable by the applications from the point of view of the iPhone's user.[74]

This case actually had a positive ending, with the courts finding that Apple the trust that consumers' had reasonably placed in its products to protect their personal data. More specifically, Apple was found to have violated the Consumer Legal Remedies Act[75] and the Unfair Competition Law.[76] Apple violated the Consumer Legal Remedies Act by not notifying its consumers that iPhones are programmed to send personal data and geographic locations to third parties unless certain settings are activated – meaning the company technically deceived its consumers.[77] Apple engaged in unfair competition by telling consumers in various ways (including marketing materials) that personal information would be kept safe and private, a deception used to increase consumer interest and sales in the iPhone.[78]

While this case likely causes some unrest in those who have Apple products, the silver lining is that Apple actually had to answer for these violations. This case shows that the law can move in a positive direction when it comes to technology and privacy. This case may have been about a company and deceptions about a physical product that were covered by the law, but the situation at hand is relatively close to the issues previously discussed concerning Facebook and online privacy.

---

[73] *Id*
[74] *Supra note 69*, 11
[75] *Supra note 69*, 70
[76] *Supra note 69*, 83
[77] *Supra note 72*
[78] *Supra note 73*

The *iPhone Application* case shows that mobile devices are not immune to the law as social media currently appears to be, and that is good news when one considers that 65 percent of Facebook users access the site daily through the mobile application.[79] As this percent rises, it shows that the window of opportunity to set online privacy laws into motion likely lies with laws concerning mobile device applications like those seen in the case just discussed.

With this window set, it is now up to the courts to set some definitions. How do you define a social media network, or what does privacy mean when one is online? As the court cases discussed in this paper demonstrate, a social media network is online, allows users to create a profile with personal data, and then allows those users to connect with and view the data of other people who have done the same. As for privacy, the definition should be simple: any data provided by or concerning the activities of a user should be considered personal and private information. Even if it is posted on Facebook, the information still belongs to the user who posted it. Therefore, consent should be required from the user in question (clear and informed consent) in order for Facebook to touch or even view this data. In the cases laid out throughout this argument, social media members have displayed the habits of treating these websites and applications as vessel through which to connect with other people. The court needs to define the purpose of social media platforms, and it would appear "vessel" is fitting – users do not expect anything to happen with their information other than a vessel sharing it with those a user chooses.

While online privacy should be the top priority, the court still needs to account for the fact that Facebook and other platforms like it are businesses that make money off of data from users. The resolution to this conflict of interest has already been established: get clear and

[79] *Supra note 68*

informed consent from users for their *depersonalized* [80] information to be shared with advertisers. This is likely in users' best interests as well so that they can continue to access Facebook without monetary expenses.

To any who would say, "If privacy is an issue, do not use Facebook at all," this option grows weaker every day. The sheer number of people logged into Facebook and other social media has made it a kind of necessity for contemporary life. Event invitations, important announcements, and other life-altering connections are commonly achieved through Facebook, LinkedIn, Twitter, Instagram, etc. It should be common knowledge in 2015 that social media is not going anywhere, if anything it is growing.[81] In this ever-evolving landscape of technology, it is incredibly important for the law to keep up.

The definitions, case studies, and window for opportunity have been laid out here for the courts. Now it is up to the U.S. legal system to play catch-up as it adapts old laws and values to the new frontier of Facebook and online privacy.

[80] See *Yunker v Pandora Media, Inc.*
[81] See Protalinski