

2014

## Facebook Messenger: Eroding User Privacy in Order to Collect, Analyze, and Sell Your Personal Information, 31 J. Marshall J. Info. Tech. & Privacy L. 393 (2014)

Erica Jaeger

Follow this and additional works at: <http://repository.jmls.edu/jitpl>

 Part of the [Computer Law Commons](#), [Consumer Protection Law Commons](#), [Internet Law Commons](#), [Privacy Law Commons](#), and the [Science and Technology Law Commons](#)

---

### Recommended Citation

Erica Jaeger, Facebook Messenger: Eroding User Privacy in Order to Collect, Analyze, and Sell Your Personal Information, 31 J. Marshall J. Info. Tech. & Privacy L. 393 (2014)

<http://repository.jmls.edu/jitpl/vol31/iss3/5>

This Comments is brought to you for free and open access by The John Marshall Institutional Repository. It has been accepted for inclusion in The John Marshall Journal of Information Technology & Privacy Law by an authorized administrator of The John Marshall Institutional Repository.

# COMMENTS

## FACEBOOK MESSENGER: ERODING USER PRIVACY IN ORDER TO COLLECT, ANALYZE, AND SELL YOUR PERSONAL INFORMATION

ERICA JAEGER\*

### I. INTRODUCTION

Facebook collects your personal data as well as website usage history.<sup>1</sup> The more personal information Facebook collects from its users; the more Facebook can profit.<sup>2</sup> Facebook has partnered with a number of data brokers in order to collect even larger quantities of personal information about Facebook users.<sup>3</sup> The collected data allows advertisers to target certain users with specific ads and sales opportunities.<sup>4</sup> Facebook is thus able to monetize users' personal information.<sup>5</sup>

Social networking sites have become information-gathering devices,

---

\* Erica Jaeger graduated from South Dakota State University in 2013 with a Bachelor of Science in Political Science and Speech Communication. Currently, Erica is pursuing her *Juris Doctor* at The John Marshall Law School, expected May 2016.

1. *What Facebook Collects and Shares*, MY SECURE CYBERSPACE, <http://www.mysecurecyberspace.com/articles/features/what-facebook-collects-and-shares.html> (last visited Jan. 24, 2015). (Website usage data is defined as the type of web browser an individual uses, the user's IP address, how long a user spends on a particular webpage, and other statistics)

2. Kim Komando, *5 Facebook details you shouldn't share*, USA TODAY (Jan. 13, 2015), <http://www.usatoday.com/story/tech/columnist/komando/2015/01/23/facebook-details-sharing/22155437/>. Facebook partnered with the Axiom, Epsilon, Datalogix, and Blue Kai to expand data collection capabilities. *Id.*

3. Kashmir Hill, *Facebook Joins Forces With Data Brokers To Gather More Intel About Users For Ads*, FORBES (Feb. 27, 2013), <http://www.forbes.com/sites/kashmirhill/2013/02/27/facebook-joins-forces-with-data-brokers-to-gather-more-intel-about-users-for-ads/>.

4. *Id.*

5. Komando, *supra* note 2.

harboring millions of peoples' personal information. Today's society strives for technological advances; however, these advances diminish an individual's online privacy. "We've been starting this trend of sacrificing privacy for features."<sup>6</sup> "They'll get over it. Just like anything else that's happened they'll get over it."<sup>7</sup> An individual's privacy online is becoming a thing of the past. Today's online technology advances at a much faster rate than society's privacy laws,<sup>8</sup> and little has been done to control it. Society has begun to accept and get over the loss of online privacy in order to advance technology. Succumbing to social networking sites' technological advances diminish the consumers' right to privacy.

Social networking sites have been exploiting consumers' personal information in order to make a profit. Facebook is one of the social networking sites, offering "a free social media platform to use and in turn sell advertising and insights based on what they learn about you."<sup>9</sup> Currently, Facebook can "collect, store and analyze data" in massive quantities.<sup>10</sup> Therefore, who protects consumers from these companies that store and sell individuals' online personal information? Is it the government's responsibility to protect consumer rights? Or is it the consumer's responsibility to limit the amount of personal information he or she offers to these companies?

Today's society focuses on what's new and convenient. However, with convenience comes sacrifice. The more convenient technology becomes; the more rights consumers lose, especially in regards to privacy. In 2013, Facebook updated its Data Use Policy, stating "We only provide data to our advertising partners or customers after we have removed your name or any other personally identifying information from it, or have combined it with other people's data in a way that it no longer personally identifies you."<sup>11</sup> Facebook gathers, collects, and analyzes an individual's data every time a user logs into Facebook, Facebook mobile, or Facebook Messenger.<sup>12</sup> So what does this mean? It means Face-

---

6. Christine VanTimmeren, *Social media outrage over Facebook Messenger App*, FOX 25 (Aug. 29, 2014), <http://www.okcfox.com/story/26237312/social-media-outrage-over-facebook-messenger-app>.

7. *Id.*

8. Vivek Wadhwa, *Law and Ethics Can't Keep Pace with Technology*, MIT TECH. REV. (Apr. 15, 2014), <http://www.technologyreview.com/view/526401/laws-and-ethics-cant-keep-pace-with-technology/>.

9. Bernard Marr, *How Facebook Exploits Your Private Information*, LINKEDIN (May 2, 2013), <https://www.linkedin.com/pulse/article/20130502052254-64875646-how-facebook-exploits-your-private-information>.

10. *Id.*

11. Anthony W. Kosner, *New Facebook Policies Sell Your Face And Whatever It Infers*, FORBES (Aug. 31, 2013), <http://www.forbes.com/sites/anthonykosner/2013/08/31/new-facebook-policies-sell-your-face-and-whatever-it-infers/>.

12. *Data Policy*, FACEBOOK, <https://www.facebook.com/about/privacy/your-info> (last visited Jan. 24, 2015).

book provides advertisers with users' data without any personal identification like the user's name or phone number; however, the information can still be linked to the user by providing companies with what area the user lives in and the user's likes or dislikes.<sup>13</sup> Facebook's new terms of service allow companies "carte blanche to guess at the details of our identities that we have not specifically disclosed and target marketing to us based on their guesses."<sup>14</sup> Today, vast amounts of consumer data can be accessed through the Internet; one can easily make 'an educated guess' and determine the true identity of those individuals. Even though, technology is advancing society, it is also crippling consumers' right to privacy.

This comment will examine Facebook's new standalone Facebook Messenger app, and review how the Privacy Policy, Data Use Policy, and the list of permissions violate Section 5 of the Federal Trade Commission Act. The comment will focus on Facebook Messenger's deceptive methods of accessing users' personal information and how Facebook uses that personal information. Section II will explain social networking sites and the configuration of Facebook, Facebook Messenger, and Facebook's evolving policies. Section II will also discuss the Federal Trade Commission and the Federal Trade Commission Act that was created to protect consumers against unfair, deceptive, or fraudulent practices.<sup>15</sup> Section III will identify Facebook's prior commitments and obligations it had to users and demonstrate how the site failed to protect users in the past. The comment will then address latent issues that arise out of Facebook Messenger's list of permissions, policies, and how it violates Section 5 of the Federal Trade Commission Act. Finally, this Comment will present a consumer-based proposal outlining the necessary changes to avoid violating Section 5 of the Federal Trade Commission Act. The proposal will address privacy and data use concerns while continuing to uphold the Federal Trade Commission Act in Facebook's day-to-day activity.

## II. BACKGROUND

### A. SOCIAL NETWORKING, THE NEXT BIG THING?

The definition of social networking is "the practice of expanding the number of one's business and/or social contacts by making connections

---

13. Kosner, *supra* note 11. "If Facebook sells a profile for 'Mr. X' to an advertiser, does it matter that my name or street address is not included if everything else about me is? They don't have to know where I live in the physical world to know where I live online." *Id.*

14. *Id.*

15. 15 U.S.C. § 45 (2010).

through individuals.”<sup>16</sup> Social networking can be an “online service, platform, or site that focuses on facilitating the building of social networks or social relations among people.”<sup>17</sup> The service enables individual users to create a profile that represents the user’s social links as well as offering a variety of additional services.<sup>18</sup> Users on social networking sites can “share ideas, activities, events, and interests within their individual networks.”<sup>19</sup> Users can interact over the Internet because a majority of “social network services are web-based.”<sup>20</sup> The sum of users on these social networking sites results in Interconnected Internet communities.<sup>21</sup>

## B. FACEBOOK

“Facebook is a social networking website that makes it easy for you to connect and share with your family and friends online.”<sup>22</sup> Users can post photos, comments, share links, and keep in touch with other Facebook users.<sup>23</sup> On February 4, 2004 “Harvard classmates Mark Zuckerberg, Eduardo Saverin, Dustin Moskovitz, and Chris Hughes” created Facebook.<sup>24</sup> Approximately 24 hours after Facebook’s creation, 1,200 Harvard students had created profiles on the site.<sup>25</sup> Within the first month of operation, half of Harvard’s undergraduate population had a Facebook user profile.<sup>26</sup> It was only a matter of months before Facebook’s network extended to all United States universities.<sup>27</sup> By September 2005, United States high school students were given access to create a Facebook profile.<sup>28</sup> Soon individuals all over the world were granted access to Facebook.<sup>29</sup> In September 2006, “the network extended beyond

---

16. Margaret Rouse, *Social Networking*, WHATIS.COM, <http://whatis.techtarget.com/definition/social-networking> (last visited Sept. 26, 2014).

17. *Social Networking*, MASHABLE, <http://mashable.com/category/social-networking/> (last visited Sept. 26, 2014).

18. *Id.*

19. *Id.*

20. *Id.*

21. Rouse, *supra* note 16.

22. *Facebook 101*, GCF LEARN FREE, <http://www.gcflearnfree.org/facebook101/2> (last visited Nov. 25, 2014).

23. Vangie Beal, *Facebook*, WEBOPEDIA, <http://www.webopedia.com/TERM/F/Facebook.html> (last visited Nov. 25, 2014).

24. Howard Koplowitz, *A Timeline Of Facebook History: From Fledgling Startup To \$114 Billion Giant*, INT’L BUS. TIMES (May 12, 2012), <http://www.ibtimes.com/timeline-facebook-history-fledgling-startup-114-billion-giant-699093>.

25. Sarah Phillips, *A brief history of Facebook*, GUARDIAN (July 24, 2007), <http://www.theguardian.com/technology/2007/jul/25/media.newmedia>.

26. *Id.*

27. *Id.*

28. *Id.*

29. *Id.*

educational institutions to anyone with a registered e[-]mail address.”<sup>30</sup> Facebook reached 100 million active users by August 2008.<sup>31</sup> Recently, as of December 31, 2014 there are 1.39 billion monthly active Facebook users.<sup>32</sup>

“Facebook’s mission is to give people the power to share and make the world more open and connected.”<sup>33</sup> Facebook users use the social networking site in order to stay connected with family and friends, as well as discovering what is happening all over the world.<sup>34</sup> Facebook allows connected users to share and express what interests them.<sup>35</sup> In April 2006, Facebook gave users the ability to access the site via mobile telephone by launching Facebook for Mobile.<sup>36</sup> “Facebook Mobile is a feature that allows a user to access Facebook from their cellphone through text messages, e[-]mails, download applications, or a web browser.”<sup>37</sup> Facebook on m.facebook.com has many features including, “posting, messaging, adding friends, uploading photos and editing your privacy settings.”<sup>38</sup>

In 2011, “Facebook launched the standalone Messenger app and rolled out some big updates in the last quarter of 2013.”<sup>39</sup> Through Facebook Messenger, users can instantly exchange chat messages with other Facebook users.<sup>40</sup> Within the Facebook Messenger app, users are capable of making voice calls, sharing photos and videos, and sending SMS text messages to other Facebook Messenger users.<sup>41</sup> Users can send and receive these messages directly from their mobile devices.<sup>42</sup> “Facebook Messenger also enables users to send chat messages to peo-

---

30. *Id.*

31. Koplowitz, *supra* note 24.

32. *Company Info*, FACEBOOK, <http://newsroom.fb.com/company-info/> (last visited Apr. 14, 2014).

33. *About*, FACEBOOK, <https://www.facebook.com/facebook/info> (last visited Sept. 26, 2014).

34. *Id.*

35. *Id.*

36. *Company Info*, *supra* note 32.

37. *Facebook Mobile*, WHATIS.COM, <http://whatis.techtarget.com/definition/Facebook-Mobile> (last visited Sept. 26, 2014).

38. *Facebook Mobile*, FACEBOOK, <https://www.facebook.com/help/121049727976363> (last visited Sept. 26, 2014).

39. Seth Fiegerman, *Facebook Plans to Launch More Standalone Apps Like Messenger*, MASHABLE (Jan. 29, 2014), <http://mashable.com/2014/01/29/facebook-standalone-apps/>.

40. *Facebook Messenger*, TECHOPEDIA, <http://www.techopedia.com/definition/28490/facebook-messenger> (last visited Sept. 26, 2014).

41. Leslie Walker, *Facebook Messenger Mobile App: Why Anyone Needs It*, ABOUT TECH., <http://personalweb.about.com/od/facebookmobile/a/Facebook-Messenger.htm> (last visited Nov. 25, 2014).

42. *Facebook Messenger*, *supra* note 40.

ple who are logged onto their Facebook accounts” via computer.<sup>43</sup> Facebook Messenger can be downloaded on the following mobile devices: Android phones, iPhones, iPads, and BlackBerry devices.<sup>44</sup> Today, iPhone and Android users are unable to send messages to other users via the Facebook application itself.<sup>45</sup> In order for Android and iPhone users to send a Facebook message, Facebook now requires users to install the standalone Facebook Messenger app.<sup>46</sup>

### C. FACEBOOK, ERODING PRIVACY ONE DAY AT A TIME.

Since Facebook’s incorporation in 2004, “Facebook has undergone a remarkable transformation.”<sup>47</sup> When it first launched, Facebook “was a private space for communication with a group of your choice.”<sup>48</sup> It was only a matter of time before Facebook “transformed into a platform where much of your information is public by default.”<sup>49</sup> Today, Facebook has become a platform that requires certain information to be made public.<sup>50</sup> Facebook can use this public information by sharing it with its partner websites in order to target specific ads at individual users.<sup>51</sup> Now, Facebook limits the amount of information users can keep private, thus shifting away from full user privacy.<sup>52</sup>

By examining Facebook’s privacy policies over the years, users can see just how Facebook transformed from a private space for communication into a more public space—shifting away from an individual’s privacy.<sup>53</sup> A privacy policy is a website’s statement regarding how specific information is collected and used.<sup>54</sup> In 2005, Facebook’s Privacy Policy stated, “No personal information that you submit to Thefacebook will be

---

43. *Id.*

44. *Id.*

45. Josh Smith, *Facebook Messenger Forced Update: What to Know*, GOTTA BE MOBILE (July 29, 2014), <http://www.gottabemobile.com/2014/07/29/facebook-messenger-forced-update-what-to-know/>.

46. *Id.*

47. Kurt Opsahl, *Facebook’s Eroding Privacy Policy: A Timeline*, ELECTRONIC FRONTIER FOUNDATION (Apr. 28, 2010), <https://www.eff.org/deeplinks/2010/04/facebook-timeline>.

48. *Id.*

49. *Id.*

50. *Id.*

51. *Id.*

52. *Id.*

53. Opsahl, *supra* note 47.

54. *Privacy Policy*, BUS. DICTIONARY, <http://www.businessdictionary.com/definition/privacy-policy.html> (last visited Oct. 19, 2014) (Defining a privacy policy as a “Statement that declares a firm's or website's policy on collecting and releasing information about a visitor. It usually declares what specific information is collected and whether it is kept confidential or shared with or sold to other firms, researchers or sellers”).

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.”<sup>55</sup> In 2007, Facebook’s Privacy Policy stated:

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.<sup>56</sup>

Facebook’s Privacy Policy as of April 2010 states:

When you connect with an application or website it will have access to General Information about you. The term General Information includes your and your friends’ names, profile pictures, gender, user IDs, connections, and any content shared using the Everyone privacy setting. ... The default privacy setting for certain types of information you post on Facebook is set to ‘everyone.’ ...Because it takes two to connect, your privacy settings only control who can see the connection on your profile page. If you are uncomfortable with the connection being publicly available, you should consider removing (or not making) the connection.<sup>57</sup>

Facebook’s current Privacy Policy as of January 2015 states, “We use the information we receive about you in connection with the services and features we provide to you and other users like your friends, our partners, the advertisers that purchase ads on the site, and the developers that build the games, applications, and websites you use.”<sup>58</sup> As the years have passed, Facebook has shifted away from complete, user driven privacy controls to limiting user privacy controls in regards to who can access users’ personal information.<sup>59</sup>

In the beginning, Facebook’s core base of users signed up because the site offered users complete control over their personal information.<sup>60</sup> However, as Facebook’s popularity grew, and the number of users drastically increased, Facebook no longer allowed users complete control of their personal information.<sup>61</sup> Instead, Facebook limited a user’s control regarding his or her personal information.<sup>62</sup> With over 200,000 million monthly users, Facebook Messenger “requires you to allow access to an alarming amount of personal data and, even more startling, direct con-

---

55. Opsahl, *supra* note 47.

56. *Id.*

57. *Id.*

58. *Data Policy, supra* note 12.

59. Opsahl, *supra* note 47.

60. *Id.*

61. *Id.*

62. *Id.*

trol over your mobile device.”<sup>63</sup> Upon downloading and using the standalone Facebook Messenger app, users are required to agree to the application’s list of permissions, which allows the app to access a variety of information on one’s mobile device.<sup>64</sup>

Facebook’s Privacy Policy also describes how third parties use users’ personal information.<sup>65</sup> Facebook is set up in a manner consistent with one’s privacy settings, but the site does not guarantee that third parties will follow Facebook’s rules.<sup>66</sup> When users share information that is set to ‘everyone’ this information is publically available.<sup>67</sup> Once the information is publically accessible, anyone with access to the Internet is capable of seeing that information.<sup>68</sup> Even individuals not logged onto Facebook can access this public information.<sup>69</sup> Publically accessible information “is subject to indexing by third party search engines and may be imported... and exported by Facebook and others without privacy limitations.”<sup>70</sup> Facebook is only responsible for its site; Facebook does not own or operate enhanced applications or websites.<sup>71</sup> So when users visit Facebook-enhanced applications and websites they are giving someone other than Facebook access to their personal information within Facebook.<sup>72</sup> In order for Facebook-enhanced applications and websites to operate at their highest capacity, “they receive publicly available information automatically when you visit them and additional

63. Sam Fiorella, *The Insidiousness of Facebook Messenger's Android Mobile App Permissions (Updated)*, HUFF. POST (Aug. 11, 2014), [http://www.huffingtonpost.com/sam-fiorella/the-insidiousness-of-face\\_b\\_4365645.html](http://www.huffingtonpost.com/sam-fiorella/the-insidiousness-of-face_b_4365645.html).

64. *Permissions*, FACEBOOK MESSENGER, <https://play.google.com/store/apps/details?id=com.facebook.orca> (last visited Sept. 27, 2014). The Facebook Messenger application is capable of: finding accounts on the device, reading your contact card, reading your contacts, finding your approximate and precise location, editing your text messages, receiving text messages, reading your text messages, sending SMS messages, directly calling phone numbers, reading call log, testing access to protected storage, modifying or deleting the contents of your USB storage, taking pictures and videos, recording audio, viewing Wi-Fi connections, reading phone status and identity, receiving data from the Internet, downloading files without notification, running at startup, preventing the device from sleeping, viewing network connections, installing shortcuts, reading battery statistics, changing your audio settings, reading Google service configuration, drawing over other apps, full network access, reading sync settings, controlling vibrations, and changing network connectivity. *Id.*

65. *Data Policy*, FACEBOOK, <https://www.facebook.com/policy.php> (last visited May 18, 2015).

66. *Terms of Service*, FACEBOOK (Jan. 31, 2015), <https://www.facebook.com/legal/terms>.

67. *Id.*

68. *Id.*

69. *Id.*

70. Opsahl, *supra* note 47.

71. *Terms of Service*, FACEBOOK (Jan. 31, 2015), <https://www.facebook.com/legal/terms>.

72. *Data Policy*, FACEBOOK, *supra* note 65.

information when you formally authorize or connect your Facebook account with them.”<sup>73</sup> In 2011, “Facebook reached a settlement agreement with the Federal Trade Commission regarding the social network’s policy on changing privacy controls and informing users of those changes.”<sup>74</sup>

The settlement requires Facebook to obtain user approval prior to “making changes to the way their personal data is shared on the network.”<sup>75</sup> “The Federal Trade Commission’s release lists seven complaints against Facebook’s allegedly deceptive privacy practices, specifically that it told users some of their personal information would be kept private, but that the site later allowed that information to become accessible.”<sup>76</sup> This type of business practice, of accessing personal information without consent, is a deceptive trade practice which is subject to examination by the Federal Trade Commission under Section 5 of the Federal Trade Commission Act.<sup>77</sup>

#### D. THE FEDERAL TRADE COMMISSION

On September 26, 1914 President Woodrow Wilson created the Federal Trade Commission (FTC), when he signed the Federal Trade Commission Act into law.<sup>78</sup> The FTC’s primary mission is to “prevent business practices that are anticompetitive or deceptive or unfair to consumers; to enhance informed consumer choice and public under-

---

73. *In Re Facebook*, EPIC.ORG, <https://epic.org/privacy/inrefacebook/> (last visited May 18, 2015).

74. Catherine Smith, *Facebook, FTC Reach Settlement Over Alleged Privacy Violations*, HUFF. POST (Nov. 29, 2011), [http://www.huffingtonpost.com/2011/11/29/facebook-ftc-reach-settle\\_n\\_1118996.html](http://www.huffingtonpost.com/2011/11/29/facebook-ftc-reach-settle_n_1118996.html).

75. *Id.*

76. *Id.* The FTC’s seven allegations are:

In December 2009, Facebook changed its website so certain information that users may have designated as private – such as their Friends List – was made public. They didn’t warn users that this change was coming, or get their approval in advance. (2) Facebook represented that third-party apps that users’ installed would have access only to user information that they needed to operate. In fact, the apps could access nearly all of users’ personal data – data the apps didn’t need. (3) Facebook told users they could restrict sharing of data to limited audiences – for example with “Friends Only.” In fact, selecting “Friends Only” did not prevent their information from being shared with third-party applications their friends used. (4) Facebook had a “Verified Apps” program & claimed it certified the security of participating apps. It didn’t. (5) Facebook promised users that it would not share their personal information with advertisers. It did. (6) Facebook claimed that when users deactivated or deleted their accounts, their photos and videos would be inaccessible. But Facebook allowed access to the content, even after users had deactivated or deleted their accounts. (7) Facebook claimed that it complied with the U.S.- EU Safe Harbor Framework that governs data transfer between the U.S. and the European Union. It didn’t.

*Id.*

77. 15 U.S.C. § 45 (2010).

78. *Our History*, FED. TRADE COMM., <http://www.ftc.gov/about-ftc/our-history> (last visited Sept. 25, 2014).

standing of the competitive process; and to accomplish this without unduly burdening legitimate business activity.”<sup>79</sup> Currently, five Commissioners govern the FTC.<sup>80</sup> The President nominates each Commissioner, and the Senate confirms the nominations.<sup>81</sup> Commissioners serve a seven-year term and “no more than three Commissioners can be of the same political party.”<sup>82</sup> One Commissioner, chosen by the president, serves as the Chairman.<sup>83</sup>

Within the FTC is the Bureau of Consumer Protection whose official order “is to protect consumers against unfair, deceptive, or fraudulent practices.”<sup>84</sup> The Bureau “enforces a variety of consumer laws enacted by Congress” as well as informing “Congress and other government entities of the impact that proposed actions could have on consumers.”<sup>85</sup> The Bureau of Consumer Protection protects consumers from “unfair, deceptive, and fraudulent business practices by collecting complaints and conducting investigations, suing companies and people that break the law, developing rules to maintain a fair market place, and educating consumers and businesses about their rights and responsibilities.”<sup>86</sup> The FTC will sue companies that make deceptive claims about their company’s products or services.<sup>87</sup>

The FTC enforces federal consumer protection laws because the Federal Trade Commission Act (FTCA) authorizes them to do so.<sup>88</sup> The FTC’s primary statute is the FTCA.<sup>89</sup> The FTC’s enforcement power originates from the FTCA.<sup>90</sup> The Federal Trade Commission Act prohibits unfair and deceptive acts and practices.<sup>91</sup> Once the FTC Board discovers unfair or deceptive acts or practices, the FTC has the authority

---

79. *About the FTC*, FED. TRADE COMM., <http://www.ftc.gov/about-ftc> (last visited Sept. 25, 2014).

80. *Commissioners*, FED. TRADE COMM., <http://www.ftc.gov/about-ftc/commissioners> (last visited Oct. 14, 2014).

81. *Id.*

82. *Id.*

83. *Id.*

84. *Bureaus & Offices*, FED. TRADE COMM., <http://www.ftc.gov/about-ftc/bureaus-offices> (last visited Sept. 25, 2014).

85. *Id.*

86. *About the Bureau of Consumer Protection*, FED. TRADE COMM., <http://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/about-bureau-consumer-protection> (last visited Sept. 25, 2014).

87. *Id.*

88. *Enforcement*, FED. TRADE COMM., <http://www.ftc.gov/enforcement> (last visited Sept. 26, 2014).

89. *Statutes Enforced or Administered by the Commission*, FED. TRADE COMM., <http://www.ftc.gov/enforcement/statutes> (last visited Sept. 26, 2014).

90. 15 U.S.C. § 45 (2010).

91. *Id.*

to take action.<sup>92</sup> “The legal standards for unfairness and deception are independent of each other; depending on the facts, an act or practice may be unfair, deceptive, or both.”<sup>93</sup> An unfair practice is when the act: “(1) causes or is likely to cause substantial injury to consumers, (2) cannot be reasonably avoided by consumers, and (3) is not outweighed by countervailing benefits to consumers or to competition.”<sup>94</sup> Depending on the circumstance “public policy, as established by statute, regulation, or judicial decisions, may be considered with all other evidence in determining whether an act or practice is unfair.”<sup>95</sup> A practice is deceptive when an act is:

(1) A representation, omission, or practice misleads or is likely to mislead the consumer, (2) a consumer’s interpretation of the representation, omission, or practice is considered reasonable under the circumstances, and (3) the misleading representation, omission, or practice is material.<sup>96</sup>

The FTC will analyze the facts and circumstances surrounding an act or practice; its finding will determine whether a particular act or practice is deceptive.<sup>97</sup>

The following section will analyze how Facebook Messenger’s policies and permissions violate Section 5 of the Federal Trade Commission Act due to the site’s deceptive business practices, in turn, leaving users’ personal information vulnerable to third party access.

### III. ANALYSIS

#### A. IN THE PAST, FACEBOOK HAS MANIPULATED AND LIED TO ITS USERS.

Facebook proclaims, “We’re committed to protecting your information. We have industry standard and proprietary network monitoring tools constantly running in our system in order to prevent security breaches and protect the security of your data.”<sup>98</sup> However, in 2011 the FTC settled charges with Facebook, stating that Facebook “deceived consumers by telling them they could keep their information on Facebook private, and then repeatedly allowing it to be shared and made

---

92. *Id.*

93. *Section 5: Unfair or Deceptive Acts or Practices*, FED. TRADE COMM. ACT, <http://www.federalreserve.gov/boarddocs/supmanual/cch/ftca.pdf>, 1 (last visited Sept. 27, 2014).

94. *Id.* at 1.

95. *Id.* at 1.

96. *Id.* at 1.

97. *Id.* at 1.

98. *What Does Facebook Do To Protect My Information*, FACEBOOK, <https://www.facebook.com/help/212183815469410> (last visited Oct. 16, 2014).

public.”<sup>99</sup> Facebook promised to keep users’ personal information private, yet broke this promise by allowing the public access to users’ private, personal information.<sup>100</sup> The FTC and Facebook reached a settlement that

Bars Facebook from making any further deceptive privacy claims, requires that the company get consumers’ approval before it changes the way it shares their data, and requires that it obtain periodic assessments of its privacy practices by independent, third-party auditors for the next 20 years.<sup>101</sup>

It would seem that as a result of the settlement, Facebook would be obligated to inform users about the sites privacy changes and how certain data is collected. Even though, Facebook notifies users of privacy changes, it does so in a deceptive manner consisting of vague and unreasonable terms, making it difficult for a reasonable Facebook user to comprehend.

In the FTC’s settlement with Facebook, Facebook agreed to a 20-year consent order in which Facebook is required to protect users’ personal information in a more explicit manner.<sup>102</sup> Facebook was ordered to comply with a multitude of provisions in order to protect users’ privacy.<sup>103</sup> The FTC’s consent order with Facebook was an administrative complaint, meaning that the FTC had “reason to believe that the law has been violated or is being violated.”<sup>104</sup> The FTC proceeded with the public’s interest at heart rather than ruling that Facebook had violated Section 5 of the Federal Trade Commission Act.<sup>105</sup> Facebook did not admit to violating the law by agreeing to the consent order; the purpose of the consent order was for a settlement resolution that would carry the force of the law in any future violations.<sup>106</sup>

---

99. Press Release, Fed. Trade Comm., Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises (Nov. 29, 2011), *available at* <http://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep>.

100. *Id.*

101. *Id.*

102. In the Matter of Facebook, Inc. (F.T.C. Jul. 27, 2012), *available at* <http://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf>.

103. *Id.* Some of the FTC orders for Facebook are as follows: Facebook was ordered not to misrepresent in any manner the extent to which it maintains the privacy or security of covered information, for Facebook to share any personal information with third-parties Facebook must clearly and prominently disclose to the user and obtain the user’s affirmative consent, Facebook must implement procedures so that third-parties cannot access user information from Facebook’s servers, Facebook shall establish a comprehensive privacy program, Facebook shall allow the FTC the ability to inspect certain documents regarding user privacy, and etc. *Id.*

104. Press Release, Fed. Trade Comm., *supra* note 99.

105. *Id.*

106. *Id.*

On the outside, it seems as if the consent order would protect Facebook users' right to privacy in regards to users' personal information. However, Commissioner Rosch's dissent in the Agreement Containing Consent Order addresses the problems of the consent order. First, the order allowed Facebook to deny all allegations set forth in the complaint.<sup>107</sup> In order for the FTC to accept the consent agreement, there needed to have been reason to believe that Facebook did in fact engage in an unfair or deceptive practice and that the consent agreement was in the interest of the public.<sup>108</sup> However, by allowing Facebook to deny all the allegations of the complaint, the requirement of "reason to believe" was not satisfied.<sup>109</sup> Rosch's second concern is that the consent order does not "unequivocally cover all representations made in the Facebook environment [while a user is on Facebook] relating to the deceptive information sharing practices of apps about which Facebook knows or should know."<sup>110</sup> Rosch gives an example of an application that a user downloaded while on Facebook.<sup>111</sup> The application within Facebook informed the user that "only me" would be allowed to see the information that the user posted and that no other users on Facebook could access the information.<sup>112</sup> Unbeknown to the consenting user, other users of the application within Facebook were capable of seeing the information that the user shared as "only me."<sup>113</sup> The FTC has not addressed concerns about these outside applications that run through Facebook's platform.<sup>114</sup> Thus, users are likely injured because Facebook does not offer users adequate disclosure when it comes to data collection.

In 2012, a study revealed that Facebook manipulated thousands of users' timelines in order to trigger an emotional response from users.<sup>115</sup> In regards to this experiment, Facebook users did not explicitly consent to take part in a study based on experimental manipulation.<sup>116</sup> Throughout the study, Facebook would "manipulate people's moods by

---

107. Dissenting Statement of Comm'r Rosch, In the Matter of Facebook, Inc., No. 0923184, 1 (F.T.C. Aug. 10, 2012), *available at* [https://www.ftc.gov/sites/default/files/documents/public\\_statements/dissenting-statement-commissioner-j.thomas-rosch-matter-facebook-inc./120810facebookstatement.pdf](https://www.ftc.gov/sites/default/files/documents/public_statements/dissenting-statement-commissioner-j.thomas-rosch-matter-facebook-inc./120810facebookstatement.pdf).

108. *Id.* at 1.

109. *Id.* at 1.

110. *Id.* at 2.

111. *Id.* at 2.

112. *Id.* at 2.

113. Dissenting Statement of Comm'r Rosch, In the Matter of Facebook, Inc., *supra* note 107.

114. *Id.* at 2.

115. Adam D.I. Kramer, Jamie E. Guillory, & Jeffery T. Hancock, *Experimental evidence of massive-scale emotional contagion through social networks*, 111 PNAS 8788-8790 (2014).

116. *Id.*

tweaking their news feeds to favor negative or positive content.”<sup>117</sup> In return, it triggered an emotional response where users wrote posts that resonated with what they had just seen or read.<sup>118</sup> Moreover, users were unaware that Facebook was going to publish users’ responses.<sup>119</sup> Even though, users did not explicitly consent to this particular study, Facebook indicated that users gave informed consent prior to creating a Facebook account when the users consented to Facebook’s Data Use Policy.<sup>120</sup>

When a user agrees to Facebook’s terms and conditions the user also agrees to Facebook’s Data Use Policy.<sup>121</sup> The Data Use Policy states that any data collected from a Facebook user’s profile is used “for internal operations, including troubleshooting, data analysis, testing, research[,] and service improvement.”<sup>122</sup> Facebook’s vague Data Use Policy and Privacy Policy allow the site to manipulate, data mine, and sell users’ personal information to third parties.<sup>123</sup> Based on Facebook’s prior actions the site has left users’ personal information vulnerable and unprotected. On multiple occasions, Facebook has proclaimed one thing, then upon further examination, and sometime later the truth is revealed,<sup>124</sup> showing that Facebook is doing the exact opposite of what it

---

117. David Talbot, *Facebook’s Emotional Manipulation Study Is Just the Latest Effort to Prod Users*, MIT TECH. REV. (July 1, 2014), <http://www.technologyreview.com/news/528706/facebooks-emotional-manipulation-study-is-just-the-latest-effort-to-prod-users/>.

118. *Id.* “Facebook ran an experiment on 689,003 users to see if it could manipulate their emotions by varying the selection of posts in their news feeds. One group had stories with positive words filtered out; another experimental group had stories with negative words filtered out. Taken as a group, the people subjected to these changes tended to write posts that echoed those moods, though the effect was small.” *Id.*

119. *Id.*

120. *Id.*

121. *Sign Up*, FACEBOOK, [https://www.facebook.com/r.php?locale=en\\_US](https://www.facebook.com/r.php?locale=en_US) (last visited Jan. 24, 2015).

122. *Data Policy*, *supra* note 12.

123. Complaint at 3, *Campbell v. Facebook Inc.*, No. C 13-5996 PJH, 2014 U.S. Dist. LEXIS 177331 (N.D. Cal. Dec. 23, 2014).

124. Press Release, Fed. Trade Comm., *supra* note 99. The FTC’s complaint stated:

Facebook allegedly made promises that it did not keep: (1) In December 2009, Facebook changed its website so certain information that users may have designated as private – such as their Friends List – was made public. They didn’t warn users that this change was coming, or get their approval in advance. (2) Facebook represented that third-party apps that users’ installed would have access only to user information that they needed to operate. In fact, the apps could access nearly all of users’ personal data – data the apps didn’t need. (3) Facebook told users they could restrict sharing of data to limited audiences – for example with “Friends Only.” In fact, selecting “Friends Only” did not prevent their information from being shared with third-party applications their friends used. (4) Facebook had a “Verified Apps” program & claimed it certified the security of participating apps. It didn’t. (5) Facebook promised users that it would not share their personal information with advertisers. It did. (6) Facebook claimed that when users deactivated or deleted their accounts, their photos and videos would be inaccessible.

first indicated. On multiple occasions, Facebook has overstepped boundaries and violated users' privacy. Facebook has exploited users' personal information in the past with minor repercussions; so now what is stopping Facebook from continuing to exploit users' personal information it collects from Facebook Messenger's list of permissions and Data Use Policy? Nothing.

#### B. VAGUE POLICIES ALLOW FACEBOOK TO DATA MINE USERS' PERSONAL INFORMATION.

In order for Facebook to protect itself from litigation, Facebook has implemented a lengthy Privacy and Data Use Policies, which are combined in multiple documents.<sup>125</sup> In regards to a user's privacy, Facebook stated that,

Your privacy is very important to us. We designed our Data Use Policy to make important disclosures about how you can use Facebook to share with others and how we collect and can use your content and information. We encourage you to read the Data Use Policy, and to use it to help you make informed decisions.<sup>126</sup>

Facebook's Privacy Policy and Data Use Policy can be found on Facebook's webpage, however, the policies span throughout a multitude of documents. This requires users to shift between several webpages in order to understand how their information is collected and what the information can be used for.

Facebook's Data Use Policy outlines the type of information the site collects and how Facebook uses that personal information.<sup>127</sup> Facebook states,

We use the information we receive about you '*in connection*' with the services and features we provide to you and other users like your friends, our partners, the advertisers that purchase ads on the site, and the developers that build the games, applications, and websites you use.<sup>128</sup>

The policy lists several examples and ways in which Facebook may use users' information, but Facebook does not provide a detailed list of

---

But Facebook allowed access to the content, even after users had deactivated or deleted their accounts. (7) Facebook claimed that it complied with the U.S.- EU Safe Harbor Framework that governs data transfer between the U.S. and the European Union. It didn't.

*Id.*

125. *Statement of Rights and Responsibilities*, FACEBOOK, <https://www.facebook.com/legal/terms> (last visited Jan. 24, 2015).

126. *Id.*

127. *Data Use Policy*, FACEBOOK, <https://www.facebook.com/policy.php> (last visited Jan. 24, 2015).

128. *Id.*

all the possible ways in which Facebook can access users' personal information.<sup>129</sup> Facebook's Data Use Policy is vague and does not represent the whole truth behind data collection. Essentially, anything Facebook deems as 'in connection with the services and features we provide' Facebook is capable of tracking, collecting, and using that user's personal information in any manner available to Facebook.<sup>130</sup> Facebook wants users to make informed decisions about using its services; however, the site reveals little information about the specifics of users' privacy rights. Since, Facebook does not offer a fully detailed list of how personal information is collected; users are left helpless and unaware of what Facebook can access.

Specifically, Facebook Messenger contains a list of permissions that allow Facebook access to a wide variety of information on a user's mobile device. "Permissions are how you ask someone if you can access that data."<sup>131</sup> Facebook Messenger has a list of thirty-two permissions which allows Facebook the ability to edit users' text messages, modify or delete the contents of users' USB storage, record audio, full network access, and etc.<sup>132</sup> The list of permissions identifies what Facebook can access, yet it fails to state the timeframe of when Facebook has access to this information and how that information is being used. The language of the list of permissions is vague and misleading, and favors Facebook rather than its users' privacy.

In Commissioner Rosch's dissent, he raised concerns that the FTC had not addressed applications that run on the Facebook platform.<sup>133</sup> Facebook Messenger's vague list of permissions is the perfect example of how the 2011 FTC settlement did not cover all of the Facebook's deceptive practices. Under Facebook's Help Center, the company addresses a few reasons behind the list of permissions.<sup>134</sup> Facebook states that allowing permissions for the application to use the user's camera and record audio are to allow "the Messenger app to easily send pictures to your friends and other contacts" or to "confirm your phone number by finding the confirmation code" within the user's text messages log.<sup>135</sup> In reality the actual list of permissions reads differently. The actual list

---

129. *Id.*

130. *Id.*

131. *Permission with Facebook Login*, FACEBOOK, <https://developers.facebook.com/docs/facebook-login/permissions/v2.1> (last visited Oct. 19, 2014).

132. *Id.*

133. Dissenting Statement of Comm'r Rosch, In the Matter of Facebook, Inc., *supra* note 107.

134. *Why is the Messenger app requesting permission to access features on my Android phone or tablet?*, FACEBOOK, <https://www.facebook.com/help/347452185405260> (last visited Oct. 19, 2014).

135. *Id.*

reads “the app has access to read your contacts...read your messages...record audio” etc.<sup>136</sup> In reality, if Facebook wanted to record audio it is authorized to do so whenever it wants, even when Facebook Messenger is not in use. Facebook also has the authority to send a text message from the user’s mobile device.<sup>137</sup> Facebook does not provide users with adequate details nor examples regarding a majority of the permissions Facebook Messenger requires.<sup>138</sup>

Within Facebook’s Help Center, Facebook explains five of the thirty-two permissions that Facebook Messenger requires.<sup>139</sup> So how does a user gain understanding of how Facebook uses the other twenty-seven permissions? This information is not available online for users. Thus, users are left vulnerable because they are unaware of how much personal information Facebook can access. Facebook has the ability to manipulate a user’s mobile device because of the vague list of permissions.

Facebook also states that it wants individual users to read through multiple documents regarding data use and privacy in order to make informed decisions about using Facebook.<sup>140</sup> The multitude of documents that Facebook requires users to shift between can confuse a user’s understanding of the site’s policies.<sup>141</sup> Confusing a user’s understanding of policies is another example of how Facebook deceives its users in order to profit off their personal information.

Facebook makes it the user’s responsibility to set individual privacy settings, because when a user fails to do so, Facebook is able to monetize accounts by selling personal information to third parties. Facebook is in the business of monetizing personal information, rather than protecting user privacy.<sup>142</sup> Overall, Facebook’s vague and minimal policies do not address the flaws regarding users’ privacy rights. The list of permissions, Data Use Policy, and Privacy Policy are deceptive to the reasonable Facebook user. When a company like Facebook says one

---

136. *Permissions*, FACEBOOK MESSENGER, *supra* note 64.

137. *Id.*

138. *Why is the Messenger app requesting permission to access features on my Android phone or tablet?*, FACEBOOK, *supra* note 134. Of the thirty-two permissions Facebook Messenger requires, Facebook only gives users examples for five of the permissions. The five examples Facebook gives give users some understanding on how Facebook uses the permissions to access user information. However, only five of the thirty-two permissions are explained to users. *Id.*

139. *Id.*

140. *Statements of Rights and Responsibilities*, FACEBOOK, <https://www.facebook.com/terms.php> (last visited Nov. 30, 2014).

141. *Campbell v. Facebook Inc.*, No. C 13-5996 PJH, 2014 U.S. Dist. LEXIS 177331 (N.D. Cal. Dec. 23, 2014) (Determining that despite the slight modifications of the language within all three policies the general principles remained the same).

142. Howard Steven Friedman, *You Are Responsible for Your Own (Facebook) Privacy*, HUFF. POST (Mar. 3, 2011), [http://www.huffingtonpost.com/howard-steven-friedman/you-are-responsible-for\\_y\\_b\\_830652.html](http://www.huffingtonpost.com/howard-steven-friedman/you-are-responsible-for_y_b_830652.html).

thing but does the opposite, an injury is likely to occur. And who bears the burden of being injured? Consumers. Facebook portrays itself as caring about user privacy and will say whatever it takes in order for users to feel at ease when using its services, like Facebook Messenger. Facebook has shifted from a social networking site that supported complete user privacy controls to limiting user privacy controls in order to data mine and monetize user's personal information by collecting, analyzing, and selling information to third parties. Facebook is deceiving users in order to make a profit at the expense of users.

The 2011 settlement between Facebook and the FTC did not cover all applications on the Facebook platform.<sup>143</sup> By allowing Facebook to deny all the allegations of the complaint, the FTC indicated that Facebook had not violated any laws.<sup>144</sup> In order for users to challenge Facebook Messenger's list of permissions and Data Use Policy, users must either wait for the FTC to step in or challenge Facebook Messenger's policies and list of permissions in court.

#### C. CAMPBELL V. FACEBOOK CHANGES THE WAY COURT'S EXAMINE CONSENT IN TERMS OF PRIVACY AND DATA USE POLICIES.

In a recent case involving the interception of Facebook users' messages, the court ruled that the plaintiffs did not impliedly consent to Facebook scanning their messages.<sup>145</sup> "Plaintiffs allege that Facebook scans the content of these private messages for use in connection with its "social plugin" functionality."<sup>146</sup> Plaintiffs further allege that Facebook scans the contents of users' messages in order to deliver users with targeted ads.<sup>147</sup> The Plaintiffs argued that Facebook violated the Federal Electronic Communications Privacy Act.<sup>148</sup> Facebook argued that under the site's Statement of Rights and Responsibilities and Data Use Policy, users expressly consented to have Facebook scan private user messages for advertising purposes.<sup>149</sup> The court noted that Facebook's Statement of Rights and Responsibilities makes no mention of scanning messages but only "encourage[s]" the reader to "read the Data Use Policy, and to use it to help you make informed decisions."<sup>150</sup> Facebook also argued that users previously consented to message scanning when the

---

143. Dissenting Statement of Comm'r Rosch, In the Matter of Facebook, Inc., *supra* note 107.

144. *Id.* at 1.

145. *Campbell*, 2014 U.S. Dist. LEXIS 177331, at \*31.

146. *Id.* at \*4.

147. *Id.* at \*4.

148. *Id.* at \*4.

149. *Id.* at \*26.

150. *Campbell*, 2014 U.S. Dist. LEXIS 177331, at \*26.

user agreed to the Data Use Policy.<sup>151</sup> Facebook's Data Use Policy states that Facebook "may use the information we received about you" for "data analysis."<sup>152</sup> However, the court ruled that these particular disclosures are "not specific enough to establish that users expressly consented to the scanning of the content of their messages."<sup>153</sup>

Additionally, Facebook claimed users impliedly consented to the alleged interceptions.<sup>154</sup> In determining implied consent, the court examined the overall circumstances and determined whether the parties had adequate notice of the interception of messages.<sup>155</sup> The court ruled that due to the lack of evidentiary record, the plaintiffs had not impliedly consented to the alleged interceptions of messages.<sup>156</sup>

Campbell is significant because the court determined that Facebook's Statement of Rights and Responsibilities and Data Use Policy were not specific enough to show that the Plaintiffs expressly or impliedly consented to the interception of personal messages without notification.<sup>157</sup> In addition, the court concluded that Facebook's disclosure statement that it "may use the information we received about you for data analysis" does not encompass the specific practice of intercepting a user's private messages.<sup>158</sup> This ruling will allow users to challenge Facebook Messenger's vague list of permissions in court, even if the FTC does not determine that Facebook violated Section 5 of the Federal Trade Commission Act.

Under Section 5 of the Federal Trade Commission Act, an act or practice is deceptive when a "representation, omission, or practice is deceptive if it is likely to mislead a consumer acting reasonably under the circumstances and is likely to affect a consumer's conduct or decision regarding a product or service."<sup>159</sup> The court's decision in Campbell and subsequent user challenges following this decision, may force the FTC to investigate Facebook Messenger's list of permissions and Data Use Policy as a possible violation of Section 5 of the Federal Trade Commission Act.

#### D. FACEBOOK MESSENGER'S LIST OF PERMISSIONS AND DATA USE POLICY IS A DECEPTIVE PRACTICE UNDER SECTION 5 OF THE FEDERAL TRADE

---

151. *Id.* at \*29.

152. *Id.* at \*28.

153. *Id.* at \*29.

154. *Id.* at \*30.

155. *Id.* at \*30.

156. *Campbell*, 2014 U.S. Dist. LEXIS 177331, at \*31.

157. *Id.* at \*26.

158. *Id.* at \*28.

159. *Unfair or Deceptive Acts or Practices by State-Chartered Banks*, FEDERAL DEPOSIT INSURANCE CORPORATION (Mar. 11, 2004), <https://www.fdic.gov/news/news/financial/2004/fil2604a.html>.

## COMMISSION ACT.

Three elements must be established to conclude that Facebook Messenger's list of permissions and Data Use Policy is a deceptive act or practice under Section 5 of the FTCA. To determine whether a representation, omission, or practice is deceptive a three-part test must be applied.<sup>160</sup> First, "the representation, omission, or practice must mislead or be likely to mislead the consumer."<sup>161</sup> Second, "the consumer's interpretation of the representation, omission, or practice must be reasonable under the circumstances."<sup>162</sup> Finally, "the misleading representation, omission, or practice must be material."<sup>163</sup>

1. Facebook Messenger's List of Permissions and Data Use Policy is a Representation, Omission, or Practice that is Likely to Mislead Consumers.

A written representation by a company can be classified as a misleading or deceptive practice.<sup>164</sup> Facebook Messenger's list of permissions and Data Use Policy is categorized as a practice. The FTC will determine if "the act or practice is likely to mislead, rather than whether it causes actual deceptions."<sup>165</sup> The FTC will evaluate a practice by determining how a reasonable consumer is likely to respond.<sup>166</sup> Prior to downloading Facebook Messenger, a user can find the list of permissions under Google Play's website.<sup>167</sup> The list of permissions is a written representation made by Facebook, and therefore qualifies as a practice under the FTCA. Thus, the first element has satisfied in determining whether an act or practice is deceptive.

---

160. *Federal Trade Commission Act Section 5: Unfair or Deceptive Acts or Practices*, FED. TRADE COMM. ACT, *supra* note 93.

161. *Id.* at 8.

162. *Id.* at 8.

163. *Id.* at 8.

164. Letter from James C. Miller III, Chairman, Fed. Trade Comm., FTC Policy Statement on Deception (Oct. 14, 1983), *available at* <http://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception> (appended to *Cliffdale Associates, Inc.*, 103 F.T.C. 110, 174 (1984)).

165. *Id.*

166. *Id.*

167. *Permissions, FACEBOOK MESSENGER*, *supra* note 64.

## 2. The Consumer's Interpretation of Facebook Messenger's List of Permissions and Data Use Policy is Reasonable Under the Circumstances.

Facebook's list of permissions and Data Use Policy is a practice that is very likely to mislead consumers. To evaluate whether a practice is likely to mislead consumers the Commission will evaluate the consumer's interpretation or reaction toward that practice.<sup>168</sup> Under this evaluation, the Commission examines how a reasonable Facebook user will interpret or react toward the permissions. If the practice misleads even a significant minority of consumers the practice will be deemed as deceptive.<sup>169</sup> In some instances, when a representation conveys more than one meaning which is likely to mislead a reasonable consumer the representation may be deceptive.<sup>170</sup> The list of permissions grant Facebook access to a wide variety of items such as access to the user's contacts within the user's mobile device all the way to the ability to change a user's network connectivity.<sup>171</sup>

Facebook's list of permissions is misleading for consumers because Facebook does not clarify when Facebook has access to the list of permissions. The list of permissions does not state when Facebook has access to the user's personal information stored on the user's mobile device. For instance, a user may believe that Facebook only has access to the list of permissions when Facebook Messenger is in use; however, Facebook's list of permission does not specify when Facebook can access a user's personal information. This is deceiving because the user may think that Facebook does not have access to his or her personal information when Facebook Messenger is not in use, but in reality Facebook may have access to the user's personal information even when the app is not in use. This is an area where Facebook's representation has two possible meanings, thus potentially placing the user in harm's way.

Facebook states that "privacy is core to our approach with Messenger, and like any developer, we analyze usage trends to make our apps better, faster, and more efficient."<sup>172</sup> However, Jonathan Zaziarski, a security researcher, revealed, "Messenger appears to have more spyware type code in it than I've seen in products intended specifically for

---

168. *Federal Trade Commission Act Section 5: Unfair or Deceptive Acts or Practices*, FED. TRADE COMM. ACT, *supra* note 93.

169. Letter from Hon. John D. Dingell, Fed. Trade Comm., FTC Policy Statement on Deception (Oct. 14, 1983), *available at* <http://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception>.

170. *Federal Trade Commission Act Section 5: Unfair or Deceptive Acts or Practices*, FED. TRADE COMM. ACT, *supra* note 93.

171. *Permissions*, FACEBOOK MESSENGER, *supra* note 64.

172. Dianne Depra, *Report claims Facebook Messenger app packed with spyware*, TECH TIMES (Sept. 21, 2014), <http://www.techtimes.com/articles/15981/20140921/report-claims-facebook-messenger-app-packed-with-spyware.html>.

enterprise surveillance.”<sup>173</sup> Even though Facebook claims the company is not collecting data with a deceptive intention, realistically the list of permissions allows Facebook to gather sensitive personal information from users who download Facebook Messenger.<sup>174</sup> Facebook’s understanding of the list of permissions is not the same as the reasonable Facebook user’s understanding. The reasonable person standard is an objective standard that examines a particular circumstance as a reasonable person would, “it is what is fit and appropriate to the end in view.”<sup>175</sup> Essentially it is “a hypothetical person in society who exercises average care, skill, and judgment in conduct and who serves as a comparative standard for determining liability.”<sup>176</sup> This is the type of standard Facebook would look to when insuring its users understand its policies. However, Facebook has not clarified all possible understandings of the list of permissions. With multiple interpretations users are left vulnerable with regard to their personal information. Numerous interpretations can mislead users’ understanding of Facebook’s policies. Thus, the second element of the deception test has been met.

### 3. Facebook Messenger’s List of Permissions and Data Use Policy Are Material.

For a representation, omission, or practice to be considered material it must be shown that “it is likely to affect a consumer’s decision regarding a product or service.”<sup>177</sup> The FTC will examine if the information is important to the consumer.<sup>178</sup> “A finding of materiality is also a finding that injury is likely to exist because of the representation, omission, sales practice, or marketing technique.”<sup>179</sup> Injury can occur in a variety of ways such as if the consumer would have chosen differently if it weren’t for the deception aspect.<sup>180</sup> Injury is likely when certain information is either inaccurate or omitted.<sup>181</sup> The FTC will find this type

---

173. *Id.*

174. Nilofar Neemuchwala, *Facebook Messenger’s Privacy Concerns Have Users Outraged*, GUARDIAN (Sept. 3, 2014) <http://guardianlv.com/2014/09/facebook-messengers-privacy-concerns-have-users-outraged/#6uokwW78Xgag8UYh.99>.

175. *Madison v. Baumann*, 162 Wis. 2d 660, 678 (1991)(citing Black’s Law Dictionary (rev. 4th ed.), p. 1431.).

176. *Reasonable Person*, LEGAL DICTIONARY, <http://legal-dictionary.thefreedictionary.com/Reasonable+person+standard> (last visited Apr. 15, 2105).

177. *Federal Trade Commission Act Section 5: Unfair or Deceptive Acts or Practices*, FED. TRADE COMM. ACT, *supra* note 93

178. Letter from Hon. John D. Dingell, Fed. Trade Comm., *supra* note 169.

179. *Id.*

180. *Id.*

181. *Id.*

of injury material.<sup>182</sup>

Facebook Messenger's list of permissions is material because in order for users to access Facebook Messenger users must agree to the list of permissions and Data Use Policy. If the Facebook user has an Android mobile device, the user must agree to all the permissions at once, whereas users with an iPhone can agree to individual permissions within the app.<sup>183</sup>

Injury occurs when users are forced into accepting all the terms of Facebook Messenger, even when the user does not understand all the terms and conditions within the Data Use Policy and list of permissions. Facebook Messenger's list of permissions and Data Use Policy does not include all of the potential examples in which Facebook can access users' personal information. Facebook omits certain crucial details regarding Facebook Messenger's list of permissions. Those omissions put the users in harm's way because the user is not fully aware of what personal information Facebook has access to. It is likely that if users knew exactly what personal information Facebook is capable of accessing through the Facebook Messenger app, the user may have chosen not to download the standalone application. Subsequently, the claim is material because the user may have come to an alternative conclusion were they fully aware of Facebook's data collection capabilities.

Under Section 5 of the Federal Trade Commission Act, Facebook Messenger's list of permissions and Data Use Policy would be considered deceptive if challenged. The FTC will be able to determine that Facebook Messenger's list of permissions and Data Use Policy qualifies as a practice. Additionally, the FTC will likely find this practice is misleading to users and is also material to the Facebook Messenger app. In return, it is likely that the FTC will determine that Facebook is involved in deceptive practices, thus violating Section 5 of the Federal Trade Commission Act.

#### E. REVAMPING FACEBOOK'S POLICIES TO CHANGE FOR THE BETTER.

The new proposal will require Facebook to explicitly identify the specifics behind Facebook Messenger's Data Use Policy, Privacy Policy, and list of permissions. The new proposal is broken down into three categories. The first category deals with terms of the Facebook's policies and list of permissions. The second category deals with notification, and the final category creates a communication system.

---

182. *Id.*

183. Reed Albergotti, *Facebook Messenger Privacy Fears? Here's What to Know*, DIGITS (Aug. 8, 2014), <http://blogs.wsj.com/digits/2014/08/08/facebook-messenger-privacy-fears-heres-what-you-need-to-know/>.

## 1. Reasonable Terms

When it comes to Facebook's privacy policies, the policies must be rewritten so that a reasonable user can understand the terms and possible consequences. With Facebook having 1.39 billion monthly active users, Facebook must rewrite the policies in plain language so that a majority of Facebook users are able to understand and comprehend the terms that are being agreed to.<sup>184</sup> As previously discussed, Facebook policies must be understood by the reasonable Facebook user. Currently, users aged 25 to 34 are the most common age demographic, accounting for 29.7% of all Facebook users.<sup>185</sup> The target demographic falls into this category, however, Facebook has an increasing number of minor children and mature users.<sup>186</sup> Thus, the changed policy terms must be rewritten so that the average, reasonable Facebook user can comprehend and understand the term's meanings. Today, Facebook's vague policies leave users vulnerable in regards to the protection of their personal information. The new proposed policy must identify the specific information Facebook Messenger can access on the user's phone. The current list of permissions are extremely vague and do not give users a fair disclosure of what types of information Facebook can access. Facebook will be required to have a well-defined and evident disclosure statement. This can be accomplished by simply requiring Facebook to state what information they can access, why access is needed, and how any collected data may be used. Users must have specifics rather than a vague and misleading list of permissions. Facebook must specify examples of all thirty-two permissions that Facebook Messenger requires, rather than defining only five. By defining all thirty-two permissions, users will have a clear understanding of what information Facebook has access to through the standalone messenger app.

After determining the exact information to be collected, Facebook creators must address when and how this information is being collected. First, the policy needs to divulge whether or not Facebook can access ones camera, text log, contacts, etc. even when the application is not in use. The application must make users aware of when Facebook has access to the information within the user's mobile device. A simple modification to the application's policies can assuage the privacy concerns that many users feel upon downloading Facebook Messenger. There must be specific examples of when Facebook is collecting data and exactly how this data is used.

---

184. *Company Info*, FACEBOOK, <http://newsroom.fb.com/company-info/> (last visited Nov. 30, 2014).

185. Dan Noyes, *The Top 20 Valuable Facebook Statistics – Updated October 2014*, ZEPHORIA (Oct. 29, 2014), <https://zephoria.com/social-media/top-15-valuable-facebook-statistics/>.

186. *Id.*

## 2. Notification

Not only must Facebook rewrite the policy terms, Facebook must be required to notify users of all policy changes in a reasonable manner. Recently, Facebook sent out a lengthy e-mail informing users that as of January 2015 the privacy policy will be changing.<sup>187</sup> Within the e-mail, Facebook states “we’re also updating our terms, data policy and cookies policy to reflect new features we’ve been working on and to make them easy to understand.”<sup>188</sup>

Facebook offers links for users to click on in order to navigate around the updated policies, however, Facebook does not point out the differences between the old and new policies. Users would have to read through the prior policies and then compare the old policies to the new in order to see how user controls have been affected. Shifting through multiple documents to understand user privacy controls is ineffective and burdensome. Facebook must be required to inform users on how the new policies differ from the prior policies in one document. This can be accomplished with a side-by-side comparison between the old and new policies. The comparison will allow users to immediately see what areas within the policies have changed and which areas have not changed. Users will find this more effective to immediately see the changes rather than having to shift through multiple documents in trying to determine where Facebook has changed its policies. With a comparison of policies, Facebook can be assured that a reasonable Facebook user is aware and understands the modifications. Due to the complexity of some changes not all users will realize and understand what each modification entails. Thus, the final revision for the proposal will require Facebook to implement a communication system.

## 3. Communication System

The final element of the new proposal is a communication system where users can acquire more details about the policies and have any questions answered in a timely fashion. Currently, Facebook directs users to a webpage called “Desktop Help” when a question arises.<sup>189</sup> Upon accessing the Desktop Help webpage, users must shift through multiple categories on a multitude of webpages to determine whether there is an answer to their question and/or problem. Solutions for all problems or questions, except data use policy questions, can only be retrieved online.

---

187. Steve Kovach, *Facebook's Privacy Policy Is Changing And You're Going To Get A Long Email About It*, BUS. INSIDER (Nov. 27, 2014), <http://www.businessinsider.com/facebook-privacy-policy-change-2014-11>.

188. *Id.*

189. *Desktop Help*, FACEBOOK, <https://www.facebook.com/help/> (last visited Nov. 29, 2014).

So when Facebook's list of pre-automated solutions does not solve or answer the user's question, the user is left with no other option than to accept Facebook the way it is or to deactivate his or her account.

When a user has a question regarding the data use policy, the user has two options for contacting Facebook. The first is through Facebook's online form where a user can type in his or her name and any additional information describing his or her data use question or concern.<sup>190</sup> The second option is to contact Facebook by mail.<sup>191</sup> When a user has a question or complaint regarding Facebook's Data Use Policy the user can write a letter to Facebook's California office or Ireland office.<sup>192</sup> However, neither of these options say if or when Facebook will answer or address the question or complaint. Requiring users to send complaints and questions via mail and online form is ineffective because it prolongs assistance. Users are left waiting for an extended period of time for Facebook to respond. This additional waiting period may cause more harm for the user if his or her privacy concern is not resolved in a timely manner. Facebook must offer users an efficient and direct line of communication.

In order to operate an efficient and direct line of communication between Facebook and users, Facebook should be required to operate a call center. Facebook's call center should operate Monday through Friday from the hours of 9am to 6pm EST. When a user calls an automated voice system would answer directing the user to push 1 for data use policy questions, push 2 for privacy policy questions, push 3 for technical questions, push 4 for general Facebook questions, and push 5 for any other Facebook orientated questions. Upon making a selection, the user would be directed to a Facebook representative that can answer any questions the user may have and explain any policies in further details so that a reasonable Facebook user can understand. The call center would provide users an immediate response to any questions or complaints that may arise upon using Facebook.

The second option within Facebook's communication system will allow users to e-mail Facebook directly. A user could communicate directly with a Facebook representative via e-mail 24/7, if the user's question

---

190. *Data Use Policy Questions*, FACEBOOK, <https://www.facebook.com/help/contact/173545232710000> (last visited Nov. 29, 2014).

191. *Data Use Policy*, FACEBOOK, <https://www.facebook.com/about/privacy> (last visited Nov. 29, 2014).

192. *Id.*

If you have questions or complaints regarding our Data Use Policy or practices, please contact us by mail. If you are located in the U.S. or Canada, our mailing address is Facebook Inc., 1601 Willow Road, Menlo Park, CA 94025. If you are located outside the U.S. or Canada, our mailing address is Facebook Ireland Ltd., 4 Grand Canal Square, Grand Canal Harbour Dublin 2, Ireland. Registered in Ireland (Companies Registration Office) Company No. 462932.

*Id.*

or complaint does not require an immediate response. There are two ways in which a user could e-mail a Facebook representative. The first option would require a user to log into his or her Facebook account and open the chat window. Within the chat window, the user could select the 'Facebook Representative' button where the user would be prompted to select a specific category depending on the user's type of question, complaint, or concern. Upon selecting a category, a text box would appear where the user can describe in detail the problem that has occurred. Once the user hits the 'Send' button an automated response would appear notifying the user that his or her message has been received and that a representative will be in contact via Facebook Chat within 48-72 hours.

The second option in e-mailing Facebook would be through the user's personal e-mail address. This option is available in case the user is not capable of accessing his or her Facebook Chat due to technical issues. On Facebook's main web page, under the 'Help' tab, Facebook would provide users with an e-mail address where concerns, questions, and problems could be directed. Within the user's personal e-mail account, the user will describe his or her problem in detail and send the e-mail to the e-mail address that Facebook has provided. Upon sending the e-mail, an automated response would be sent verifying that the previous e-mail has been received and that a Facebook representative will be in contact via personal e-mail within 48-72 hours. Between the call center and e-mail options Facebook users will now have the option to communicate with Facebook directly in a more efficient manner.

The new proposal would be implemented in order to safeguard Facebook users from the fraud, deception, and unfair business practices that Facebook implements. Facebook has the obligation to uphold users' privacy rights, and if Facebook disregards consumer's rights the Federal Trade Commission has the authority to act. The Federal Trade Commission has authority under Section 5 of the FTCA in order to "protect consumers by stopping unfair, deceptive, or fraudulent practices in the marketplace."<sup>193</sup>

Throughout this Comment it has been established that Facebook Messenger's lists of permissions and policies have violated Section 5 of the Federal Trade Commission Act. This Comment has discussed a possible legal solution, which would better safeguard users' privacy rights and gives adequate notice for when Facebook modifies data use and privacy policies. As stated earlier, for years consumers' rights have been placed on the back burner and sacrificed in order to advance technology. Privacy laws must advance with today's changing technology; otherwise consumers will constantly be the ones paying the price, until eventually

---

193. *What We Do*, FED. TRADE COMM., <http://www.ftc.gov/about-ftc/what-we-do> (last visited Oct. 19, 2014).

consumer privacy is completely eradicated due to a company's wordy privacy policy.

#### IV. CONCLUSION

In today's society where a majority of individual's post intimate details about his or her life on social network sites, one would think that individuals would have control over who has access to their personal data, however, that is not the case. Today, privacy is becoming a thing of the past. Facebook Messenger's list of permissions, Data Use Policy, and Privacy Policy mislead consumers into thinking their privacy is being protected. Facebook's Data Use Policy and Privacy Policy are multiple pages filled with vague and misleading terms. Anything Facebook deems "in connection with the services and features we provide" they are able to track, collect, and use in any manner available to Facebook.<sup>194</sup> So when does a user know Facebook has deemed something "in connection with its services and features?" Facebook does not offer this information publically, the only way to find what is in connection with Facebook is through an internal information leak, at which point the information will have been collected and the injury sustained. Facebook's policies are vague and misleading, which leads to one thing—consumers being left vulnerable and unprotected.

Facebook's Data Use Policy and Privacy Policy must be condensed and rewritten to facilitate a reasonable user's understanding. Currently, Facebook has a 14,000-word term of service and data use policy.<sup>195</sup> Facebook's policies, in comparison to Snapchat, Twitter, and Instagram contain significantly more text. Twitter's privacy policy has 2,151 words,<sup>196</sup> Instagram's about 2,000 words and Snapchat's approximately 1,800 words.<sup>197</sup> Facebook's policies and terms of service tower over other social networking sites. In order to better inform users, Facebook must restructure its policies.

This Comment discussed Section 5 of the Federal Trade Commission Act and how Facebook violated the Act due to the company's deceptive practices. This Comment addressed a solution where consumer rights are being advanced rather than corporate data collection, and the

---

194. *Data Use Policy*, FACEBOOK, [https://www.facebook.com/full\\_data\\_use\\_policy](https://www.facebook.com/full_data_use_policy) (last visited Oct. 19, 2104).

195. Oliver Smith, *Facebook terms and conditions: why you don't own your online life*, TELEGRAPH (Jan. 4, 2013), <http://www.telegraph.co.uk/technology/social-media/9780565/Facebook-terms-and-conditions-why-you-dont-own-your-online-life.html>.

196. *Number of words in the privacy policies of selected social networks as of 2012*, STATISTIC, <http://www.statista.com/statistics/268079/privacy-policy-word-count-of-selected-social-networks/> (last visited Nov. 4, 2014).

197. Ashley T. Powell, *Shorter privacy policies win-win for all*, THE DAILY WILDCAT (Oct. 28, 2013), <http://www.wildcat.arizona.edu/article/2013/10/shorter-privacy-policies-win-win-for-both-users-companies>.

proposal was designed to place Facebook users on notice and give them the opportunity to understand all policy modifications in layman terms rather than advanced legalese. Technology is advancing at a much faster rate than consumer privacy laws. If the FTC does not hold companies, like Facebook, accountable for their breaches of privacy rights, they continue to quash user privacy controls until privacy no longer exists, leaving privacy rights a thing of the past.