Consumers' Obsession Becoming Retailers' Possession: The Way That Retailers Are Benefiting from Consumers' Presence on Social Media

VIVIAN ADAME*

TABLE OF CONTENTS

 J.D. 2017 Candidate, University of San Diego School of Law; B.A. 2014, Communication, San Diego State University. I dedicate this Comment to my family for their support and gratefully acknowledge the *San Diego Law Review* editorial board for affording me this opportunity. I would also like to thank my Faculty Advisor, Professor Jane Henning, and my Comments Editor, Madison Levine. Both guided me throughout the drafting process.

I. INTRODUCTION

During a break from work, you decide to check your social media page for some entertainment. To your delight, you discover that your cousin decided to propose to his girlfriend on the Great Wall of China, your best friend received a promotion, and Lululemon posted your recent Instagram Scorpion Pose photo on its website.[1] You then decide to quickly check

1. *See Who is Lululemon Athletica?*, LULULEMON ATHLETICA, http://www.lululemon.com/about [https://perma.cc/EEB6-ZL7C] (last visited Aug. 4, 2016) (describing Lululemon Athletica as a yoga-inspired apparel company, which produces clothing meant to be the

on flights to London for that trip to Europe you are planning. Upon returning to your social media page just before your break is over, you realize that all of the ads on your social media feed now feature deals on flights around the world. Although you are not sure how Instagram knows that you are interested in traveling to Europe, you decide that it is time to get back to work.[2]

Social media sites have become avenues where retailers and brands can capitalize on consumers' social media presence.[3] Companies can use these sites as marketing tools to personalize their brands and encourage consumer engagement.[4] However, due to the mainstream use of social media and the need to stay present, many consumers are oblivious to the fact that they are giving up a great deal of private information about themselves by simply creating a profile on social media. The more chilling fact is that social media companies make billions of dollars by selling users' information to retailers who are eager to collect it.[5] Social media companies collect users'

---

perfect combination of supportive and flexible material, providing people with "components . . . to live long, healthier, fun lives"); Ann Pizer, *Scorpion Pose - Vrschikasana*, VERY WELL, https://www.verywell.com/scorpion-pose-vrschikasana-3567113 [https://perma.cc/44B3-XFRT] (last updated Dec. 29, 2015) (explaining that Scorpion Pose is an inverted backbend that is held while holding a handstand or forearm stand). "The Sweat Life" is Lululemon's ongoing campaign intended to promote its products by featuring images of Lululemon's social media followers who have uploaded photos of themselves wearing Lululemon products using #thesweatlife or #Lululemon to connect their photos to the brand. *See Living #thesweatlife*, LULULEMON: THE BLOG (Feb. 23, 2013), http://blog.eu.lululemon.com/living-thesweatlife/ [https://perma.cc/D56C-YCVH]. Lululemon then chooses flattering photos from its followers' posts and uploads these photos to the company's website. *Id.*

2. When Instagram first introduced advertisements to its social media site, it only allowed brands who had a successful Instagram following to advertise their posts. *See* Olsy Sorokina, *Instagram Ads: Everything You Need to Know*, HOOTSUITE: SOC. BLOG (Nov. 8, 2014), http://blog.hootsuite.com/everything-you-need-to-know-instagram-ads/ [https://perma.cc/P2KT-5JKG]. Instagram aimed "to make any advertisements [users saw] feel as natural to Instagram as the photos and videos many [users] already enjoy[ed] from [their] favorite brands." *Id.*

3. In 2013, sales on Facebook and Pinterest alone totaled over 56% of social generated e-commerce. *See* Cooper Smith & Marcelo Ballve, *The Rise of Social Commerce—How Tweets, Pins and Likes Are Driving Sales, Online and Offline*, BUS. INSIDER (Aug. 6, 2013, 4:30 PM), http://www.businessinsider.com/social-commerce-and-retailer-benefits-2013-8 [https://perma.cc/WVC3-BR9J] (discussing the positive economic impact that increased social media use has had on retailers).

4. *See* Danielle McKelley, *What Does a #Hashtag Mean in Social Media?*, WAYPOST (Jan. 29, 2015), http://blog.waypostmarketing.com/what-does-a-hashtag-mean-in-social-media [https://perma.cc/ZR9M-QRVQ].

5. PHILIP M. NAPOLI, AUDIENCE ECONOMICS: MEDIA INSTITUTIONS AND THE AUDIENCE MARKETPLACE 2–3 (2003).

information whenever they post a picture, comment on a friend's status, or even just create a dormant social media profile.[6] Although retailers have profited from consumer information ever since the Internet began to fuel commercial growth, the development of social media has exacerbated this problem; sites like Facebook, Instagram, and Twitter serve as avenues to collect extensive amount of personal information, which is then sold to retailers. Thus, social media has become a "dual market" that simultaneously allows retailers to sell products to users and allows social media sites to sell their audiences to retailers at the expense of users' privacy.[7]

The majority of global retailers have established some sort of presence on social media.[8] Some of these retailers not only share their new merchandise, products, and updates with social media followers, but also create an online personality for their company—allowing them to personally engage with their social media followers.[9] Brands that engage their followers on social media use the hashtagged[10] photos their users post as

6. According to a recent study conducted by *Business Insider Intelligence*, social media users are no longer predominately millennials; the study revealed that over 50% of individuals over sixty-five in the United States used some sort of social media site. *See* Mona Zhang, *Social Networking Has Officially Gone Mainstream*, SOC. TIMES (Sept. 2, 2014, 9:59 AM), http://www.adweek.com/socialtimes/social-networking-officially-gone-mainstream/203850 [https://perma.cc/FT7E-PHDT].

7. *See* James G. Webster, *User Information Regimes: How Social Media Shape Patterns of Consumption*, 104 NW. U. L. REV. 593, 598 (2010); NAPOLI, *supra* note 5.

8. Research has shown that at least 80% of the top fifty global brands, which include Gap, J.Crew, American Eagle, Victoria's Secret, and Coach, among others, maintain an active social media presence on top sites like Facebook, Twitter, Instagram, Pinterest, and LinkedIn. *See* Greg Beaubien, *Users Tuning Out Social Media Posts from Brands*, PUB. REL. SOC'Y OF AM. (Aug. 27. 2015), https://www.prsa.org/SearchResults/view/11184/105/Users_Tuning_Out_Social_Media_Posts_from_Brands#.VfB2YXhX9FI [https://perma.cc/CF5N-67TN]; Barbara Thau, *Interbrand Reveals 'Best Retail Brands' of 2014 (And the Biggest Losers)*, FORBES (Apr. 8, 2014, 8:00 AM), http://www.forbes.com/sites/barbarathau/2014/04/08/interbrand-reveals-the-best-retail-brands-of-2014-and-the-biggest-losers/ [https://perma.cc/QV9E-U9UA].

9. Starbucks is a prime example of a company that was more than successful in using social media to establish an engaging platform; its users benefitted more from the information the company shared. Because Starbucks responds to each and every tweet it receives from a consumer, its engagement with social media users contributes highly to its success on social media. *See* Robert Gembarski, *How Starbucks Built an Engaging Brand on Social Media*, BRANDING PERSONALITY, http://www.brandingpersonality.com/how-starbucks-built-an-engagin-brand-on-social-media/ [https://perma.cc/DZW3-QL3F] (last visited Aug. 4, 2016).

10. One man, Christopher Messina, can be credited for the idea of the hashtag (#), which he first proposed to Twitter on his blog by stating that he was "more interested in simply having a better eavesdropping experience on Twitter." Alexis C. Madrigal, *The Hashtag is About to Roll Out to a Billion People, and This One Guy Invented It*, ATLANTIC (June 12, 2013), http://www.theatlantic.com/technology/archive/2013/06/the-hashtag-is-about-to-roll-out-to-a-billion-people-and-this-one-guy-invented-it/276811/ [https://perma.cc/G5AP-K8BN]. "He imagined that each hashtag would create a (temporary) channel,

a free marketing tool because social media users wish to be featured on the brand's website or social media page.[11] Thus, in this day and age where over 1.4 billion people have a Facebook profile, 300 million people have an Instagram account, and 2.8 billion people have a Twitter account, retailers have a huge audience they can market to by creating an engaging social media presence.[12]

Retailers can profit from consumers' social media presence in two ways: (1) through inadequate privacy laws; and (2) through retailers' reposting of consumers intellectual property uploaded to social media sites.[13] The

analogous to an IRC (Internet Relay Chat) channel," which could be used to identify topics, ideas, or messages. *Id.* Today, the hashtag is used to mark keywords or topics in a Tweet, Facebook post, or Instagram post. *Id.* On Twitter, if a user Tweets from a public account, anyone who does a search for that hashtag may find their Tweet. *Using Hashtags on Twitter*, TWITTER, https://support.twitter.com/articles/49309 [https://perma.cc/6BH9-F9U8] (last visited Aug. 4, 2016).

11. *See, e.g.*, *Living #thesweatlife*, *supra* note 1; J.Crew (@jcrew), INSTAGRAM, https://instagram.com/jcrew/ [https://perma.cc/64NV-TXFN] (last visited Aug. 4, 2016); Urban Outfitters (@urbanoutfitters), INSTAGRAM, https://instagram.com/urbanoutfitters/ [https://perma.cc/HA3H-TK27] (last visited Aug. 4, 2016).

12. These numbers reflect the social media sites' active users; the total number of social media users, including those with dormant profiles, is higher. *Social Networking Statistics*, STATISTIC BRAIN, http://www.statisticbrain.com/social-networking-statistics/ [https://perma.cc/U2GG-R3Y2] (last updated Dec. 1, 2015).

13. While retailers' use of users' intellectual property on social media is a prominent way that retailers are benefitting from consumers' presence on sites like Facebook, Instagram, and Twitter, this Comment will focus on the privacy rights issue. However, if the legislature were to implement a new law geared toward regulating the terms of use and privacy policies of social media sites, such a law could potentially resolve the problem of retailers profiting from the use of social media users' intellectual property. Recently, Facebook was sued for using photos of minors for its own advertisements, without the consent of the minors' parents; the company proposed a $20 million settlement to resolve the dispute. *See* Joe Van Acker, *Facebook's $20M Privacy Deal Is Illegal, Dad Tells 9th Circ.*, LAW360 (Jan. 21, 2016), https://advance.lexis.com/document/?pdmfid=1000516&crid=f57c4670-6389-4402-821f-0f2f8649fe7a&pddocfullpath=%2Fshared%2Fdocument%2Flegalnews%2Furn%3AcontentItem%3A5HX6-8CH1-F22N-X4TP-00000-00&pddocid=urn%3AcontentItem%3A5HX6-8CH1-F22N-X4TP-00000-00&pdcontentcomponentid=122080&pdteaserkey=sr0&ecomp=7nLhk&earg=sr0&prid=618435f4-f6e5-405a-811b-f18b7ea1d0cc [https://perma.cc/JJ2N-Y4GK]. According to the plaintiff, "[t]he settlement agreement purports to delegate to Facebook unfettered power to take information posted by a child, package it, and transmit it in any form and to potentially millions of recipients and for any commercial purpose, as Facebook determines . . . ." *Id.* Professor Robert Fellmeth, Executive Director of the Center for Public Interest Law and Children's Advocacy Institute at the University of San Diego School of Law, is serving as counsel for the plaintiff. As Professor Fellmeth stated, the Ninth Circuit must review its decision upholding the validity of Facebook's settlement proposal, otherwise "[i]f this decision stands, it will have long standing consequences all of the justices will regret" because the unpublished decision

California Legislature passed the Online Privacy Protection Act (CalOPPA), which moved towards protecting the privacy rights of consumers.[14] However, the Legislature's inability to hold retailers accountable under CalOPPA leaves consumers susceptible to the invasive technologies retailers use to collect social media users' information, which they in turn sell and profit from.[15] To better protect consumers on social media, the legislature should first enact a privacy law restricting retailers' and social media sites' use of invasive technologies to collect and sell social media users' personal information. The legislature must require all businesses to abide by a consumer's request to opt-out of being tracked online.

Part II of this Comment will explain how social media has created new ways for retailers to profit from online users' private information. Part III will analyze the legal responses to the online privacy issue in terms of legal opinions and legislative attempts to protect the privacy of online consumers. Because social media sites provide retailers with massive amounts of personal and often private information from unsuspecting users, Part IV advocates for a privacy law that requires social media sites and retailers to honor the privacy requests of social media users. Lastly, Part V advocates for Congress to act on the proposed Consumer Privacy Bill of Rights Act (CPBRA) and dedicate a section of the bill to the regulation of social media sites' and retailers' use of consumer information.[16]

II. THE EXPANSION OF THE INTERNET AND THE REALM OF SOCIAL MEDIA

The commercial development of the Internet has changed the way that members of society interact, conduct business, and keep in touch. In turn, while the Internet has become an integral part of society, certain advancements in technology have allowed retailers to prosper from the

---

will "remove the basic child and parental privacy rights directly applicable to over 10 million American teens." *Id.*

14. *See* Press Release, Cal. State Senator Joe Simitian, Bill to Protect Privacy of Web Surfers To Be Heard Tomorrow in Assembly Committee (May 6, 2002), http://www.senatorsimitian.com/entry/bill_to_protect_privacy_of_web_surfers/ [https://perma.cc/4S7X-A5KU] ("My goal here is simple . . . [m]ake sure online users know what their privacy protections are. Make sure those guarantees are honored."); *infra* Section III.B.1.

15. Because CalOPPA only provides consumers with enough information to determine whether they want to engage in online commerce with businesses that collect their personal information, the Act does not provide users with a remedy if they want to prevent retailers from using their personal information. Although CalOPPA's scope covers the privacy of consumers on any site online, this Comment will focus strictly on its application to social media sites. *See infra* Section III.B.1.

16. *See* WHITE HOUSE, ADMINISTRATION DISCUSSION DRAFT: CONSUMER PRIVACY BILL OF RIGHTS ACT OF 2015 [hereinafter CONSUMER PRIVACY BILL OF RIGHTS ACT OF 2015]; *infra* Section IV.B.

lack of privacy laws geared toward protecting consumers' online information. The development of social media has only intensified this problem as retailers find new ways to track very detailed and specific information about users.

A. Discovering Why Search Engines and Social Media Sites Seem to Know About Your Tastes and Interests

The Internet has been referred to as "the fastest-growing medium in human history" because the majority of the population uses it in every aspect of their daily lives.[17] Thus, it is no surprise that web providers and search engines quickly realized the propensity for profit that a massive audience can provide.

1. A Cookie for Your Thoughts? The Nature of Behavioral Advertising

Search engines like Google, Yahoo, AOL, and MSN all offer their users free web searching services because they intend to sell their audience to retailers who pay for Internet advertising.[18] Because individuals submit information to companies like Google, Yahoo, AOL, and MSN, through their queries, search engines collect a vast amount of information that "represents a massive clickstream database of desires, needs, wants, and preferences that can be discovered, subpoenaed, archived, tracked, and exploited."[19] Search engines collect information from Internet users through the use of cookies.[20]

Social media sites, like all other websites, can install first-party cookies on the computer of any user who accesses the site.[21] A first-party cookie is a file issued by the host website a user is accessing that, once saved on

17. *See* Christopher F. Carlton, *The Right to Privacy in Internet Commerce: A Call for New Federal Guidelines and the Creation of an Independent Privacy Commission*, 16 ST. JOHN'S J. LEGAL COMMENT. 393, 394 (2002) (discussing the widespread use of the Internet and the fact that many citizens have become weary of their inability to protect privacy and information online).

18. *See* Ira S. Rubinstein et al., *Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches*, 75 U. CHI. L. REV. 261, 271–72 (2008).

19. *See id.*; JOHN BATTELLE, THE SEARCH: HOW GOOGLE AND ITS RIVALS REWROTE THE RULES OF BUSINESS AND TRANSFORMED OUR CULTURE 6 (Penguin Books 2006) (2005).

20. The use of cookies as a means of tracking Internet users' behavior first sparked privacy complaints in the late 1990s, but it has since been a debate that has not favored consumers. *See* Rubinstein et al., *supra* note 18.

21. *See Cookies & Other Storage Technologies*, FACEBOOK, https://www.facebook.com/help/cookies/ [https://perma.cc/H4K2-SXAE] (last visited Aug. 4, 2015).

the user's computer, tracks the user's activity as they navigate that website.[22] Thus, Facebook, Instagram, and Twitter can keep track of each user's activity as they browse through different pages on the social media sites.[23] Although first-party cookies often provide social media users with a better experience because they allow websites to remember users, these cookies could convey sensitive information to social media sites like an individual's location, searches they have conducted, and the pages they have visited while online.[24] Additionally, one of the biggest risks that first-party cookies pose is the threat of hackers obtaining users' login information.[25]

According to Instagram's Privacy Policy, the company "may share User Content and your information (including but not limited to, information from cookies, log files, devices, identifiers, location data, and usage data)" with third-party organizations and third-party advertisers that have no direct affiliation with the site.[26] Additionally, as stated in Instagram's Terms of Use, the social media site attempts to relieve itself of any liability regarding information that may be shared if consumers interact with third-parties found on Instagram; these third-parties include retailers' websites.[27] Instagram states in all caps, "YOUR CORRESPONDENCE AND BUSINESS DEALINGS WITH THIRD PARTIES FOUND THROUGH THE SERVICE ARE BETWEEN YOU AND THE THIRD PARTY."[28] Consumers who interact with these third parties risk unknowingly sharing their profile information and allowing "personally identifying information to be publicly disclosed and/or associated with [them], even if Instagram has not itself provided such information."[29]

---

22. First-party cookies can also make logging onto the social media sites and other web accounts easier because they allow the websites to remember the username and password of a user, eliminating the need to login every time they access the site. Benjamin Strauss, *Online Tracking: Can the Free Market Create Choice Where None Exists?*, 13 CHI.-KENT J. INTELL. PROP. 539, 540 (2014).

23. *See id.*

24. These types of cookies are both useful and convenient for social media users because they allow websites to remember their usernames and passwords. *See id.*

25. *Id.*

26. *See Privacy Policy*, INSTAGRAM, https://instagram.com/about/legal/privacy/ [https://perma.cc/JL25-L8LR] (last visited Aug. 4, 2016) [hereinafter *Instagram Privacy Policy*].

27. *See Terms of Use*, INSTAGRAM, https://help.instagram.com/478745558852511 [https://perma.cc/7J3M-XGU5] (last visited Aug. 4, 2016).

28. *Id*.

29. *Id*. In 2012, Facebook acquired Instagram for $1 billion in cash and stock, which resulted in Instagram's controversial terms of use. Nicole Cocozza, *Instagram Sets a Precedent by an "Insta" Change in Social Media Contracts & Users' Ignorance of Instagram's Terms of Use May Lead to Acceptance by a Simple "Snap,"* 15 J. HIGH TECH. L. 363, 364 (2015). Instagram's Terms of Use, like the terms of use of other social media sites, allows Instagram to have some control over the personal freedom of its users, who must agree if they want "to live and participate in a world steeped in social media." *Id.* at 365. Moreover, Instagram explicitly states that its "Terms of Use affect your legal rights

Instagram seeks to relieve itself of any liability when users interact with retailers and other third parties because once a user even clicks a retailer's advertisement, a more significant amount of information is likely to be conveyed; retailers can then use this information to their advantage in the future.[30] On its business blog, Instagram stated: "Instagram ads have proven to drive strong branding results—97% of measured campaigns . . . have generated significant lifts in ad recall."[31] With such a high success rate, retailers and other advertisers have an incentive to pay social media sites like Instagram, Facebook, and Twitter to obtain the information the sites collect. Users' information gives retailers the opportunity to market products to fans of the brand and target new audiences likely to become new fans, further allowing them to profit off of the personal information each user may unknowingly provide.[32]

Facebook also takes advantage of first-party cookies by tracking what users "Like" as well as the searches they conduct on the site.[33] Of course, although retailers and Facebook profit from tracking users' every move on the social media site, this business venture is sold to consumers as allowing marketers to "reach the right groups of people with the right message and drive the results they most care about."[34] For consumers, this means that Facebook will happily sell the information that its first-party cookies have collected to make a huge profit.[35] Social media users should ask themselves

---

and obligations . . . [i]f you do not agree to be bound by all of these Terms of Use, do not access or use [Instagram]." *See Terms of Use*, *supra* note 27.

30. *See Terms of Use*, *supra* note 27.

31. *Instagram: Open to Businesses of All Sizes, Everywhere*, INSTAGRAM: INSTAGRAM FOR BUSINESS (Sept. 2015), http://blog.business.instagram.com/post/128686033016/150909-advertisinglaunch [https://perma.cc/5QGV-6QQP].

32. *See* Peter Roesler, *5 Benefits of Social Media Business Owners Need to Understand*, INC. (Sept. 8, 2014), http://www.inc.com/peter-roesler/5-benefits-of-social-media-business-owners-need-to-understand.html.

33. *See Cookies & Other Storage Technologies*, *supra* note 21.

34. *See* Fidji Simo, *An Update on Facebook Ads*, FACEBOOK: NEWSROOM (June 6, 2013), http://newsroom.fb.com/news/2013/06/an-update-on-facebook-ads/ [https://perma.cc/YJ6Y-3G7P] (discussing how Facebook advertisements work and whether Facebook uses personal information when creating its ads). Your profile picture can even be used to promote ads on Facebook since the site can associate your name and picture next to retailers' pages that you have liked, though this information is only displayed to those who are allowed to view your personal profile. *See About Advertising on Facebook*, FACEBOOK, https://www.facebook.com/about/ads/ [https://perma.cc/MF3E-4GSE] (last visited Aug. 4, 2016).

35. In 2014, Facebook had made over $3.2 billion in revenue from advertisements. Tim Peterson, *Facebook's Closed the Mobile Gap, but What About the Google Gap?*,

if having free access to social media sites like Facebook, Instagram, and Twitter is worth losing their privacy.[36] Considering the benefits that any social media user reaps by creating a profile on Facebook, Instagram, Twitter, or the like, many consumers would find that paying to use these services is worth the money spent.[37] In particular, by paying any amount of money to use these services, a social media user could sue a social media site if the company breached its duty to adhere to the contract that a user agrees to when it registers for a social media account.[38] However, because social media sites will continue to be free, Congress must implement a federal privacy law that requires social media sites to have better terms for users in order to better protect social media users from retailers and social media sites profiting off of their private information.[39]

This new law would be of particular importance because social media sites do not stop tracking users once they have left the site.[40] Facebook tracks its users when they "visit or use third-party websites and apps that use [Facebook's] Services"; third-party websites use Facebook's "Services" anytime they feature Facebook's "Like" button, log in, or use Facebook's advertising services.[41] The third-party websites and applications (apps) that are "integrated with" Facebook "may receive information about what [users] post or share."[42] Facebook also has a "family of companies that are part of

---

ADVERT. AGE (Oct. 28, 2014), http://adage.com/article/digital/facebook-makes-66-money-mobile-ads/295616 [https://perma.cc/2CSR-XK67].

36. Social media sites and other services, including Google, are ad-financed Internet platforms—they make money because advertisers pay for access to these sites' user databases. *See* Zeynep Tufekci, *Mark Zuckerberg, Let Me Pay for Facebook*, N.Y. TIMES (June 4, 2015), http://www.nytimes.com/2015/06/04/opinion/zeynep-tufekci-mark-zuckerberg-let-me-pay-for-facebook.html?_r=0.

37. *See* Tim Wu, *Facebook Should Pay All of Us*, NEW YORKER (Aug. 14, 2015), http://www.newyorker.com/business/currency/facebook-should-pay-all-of-us [https://perma.cc/Y7WZ-B4AR].

38. *See infra* Section III.A.

39. Rumors that social media sites like Facebook would start charging its users have become prominent over the years, but are false nonetheless. *See* Adam Ostrow, *Facebook Will Never Charge You to Use It. Here's Why*, MASHABLE (Sept. 29, 2011), http://mashable.com/2011/09/29/facebook-pay/#GQL_WKwW4uq6 [https://perma.cc/6H3J-TS2B]. Social media sites will continue to be free because they become more profitable with the more users they have; Facebook, like other social media sites, makes money "on highly targeted advertising that's based on the plethora of data that its members share on the site. Restricting users' ability to use the site would actually be detrimental to that model." *Id.*

40. *Data Policy*, FACEBOOK, https://www.facebook.com/policy.php [https://perma.cc/5M2G-DJXJ] (last updated Jan. 30, 2015) [hereinafter *Facebook Data Policy*].

41. *Id.*

42. *Id.* Facebook allows its users to "opt to express their views by engaging with content created by others" through their use of "social sharing buttons." Alicia D. Sklan, Note, *@SocialMedia: Speech with a Click of a Button? #SocialSharingButtons*, 32 CARDOZO ARTS & ENT. L.J. 377, 379 (2013). For example, if a social media user were to enjoy an article featured on The Huffington Post, social sharing buttons would allow the

Facebook" with which it shares user information, including their username, email, and all activity that a user conducts while using the site.[43] Facebook shares this information with its family companies to "facilitate, support and integrate their activities and improve [their] services."[44] At least one of Facebook's family companies, Atlas, is an advertising company that collects information from all Facebook users' "browsers and devices when [they] or others using their browser or device view, visit, or use advertisements, websites or apps that use [the Facebook family companies'] Services."[45] However, Atlas's tracking and collection of Facebook users' information does not stop there: Atlas also collects "information from third parties such as [their] customers and partners, which include marketing partners, publishers, and service providers, related to their use and support" of Atlas' advertising services.[46]

Facebook insists that it does not provide third parties with personally identifiable information such as a user's name or email address.[47] However, a review of Atlas's privacy policy shows that Facebook shares this information with family companies like Atlas, who may in turn share that information with other third parties.[48] Additionally, even if Facebook did not sell personally identifiable information to third-party advertisers or share this information with its family companies, the third parties and family companies would already have obtained so much information about a user that their name would be irrelevant. For example, because family companies and third parties would already know a user's likes, dislikes, and activities on apps, these companies do not need a user's exact name to exploit their

user to "like" or "share" the article on Facebook, "favorite" it on Instagram, "tweet" it on Twitter, or "pin" it on Pinterest. *Id.* Thus, social media users are not limited to their own posts, but may "like" content posted by others obtained outside the social media realm. *Id.* On Facebook, users can also interact by playing apps and games through the social media site, such as Clash of Clans, Texas HoldEm Poker, and Bejeweled Blitz. *About Apps*, FACEBOOK, https://www.facebook.com/help/493707223977442/ [https://perma.cc/SG5N-F5XH] (last visited Apr. 9, 2016).

43. The companies within the Facebook Family include Facebook Payments, Atlas, Instagram, Onavo, Parse, Moves, Oculus, LiveRail, and WhatsApp. *See The Facebook Companies*, FACEBOOK, https://www.facebook.com/help/111814505650678 [https://perma.cc/DNP3-SEEW] (last visited Aug. 4, 2016).

44. *Id.*

45. *Privacy Policy*, ATLAS BY FACEBOOK, http://atlassolutions.com/privacy-policy/ [https://perma.cc/7WDJ-AXDN] (last visited Aug. 4, 2016) [hereinafter *Atlas Privacy Policy*].

46. *See id.*

47. *Facebook Data Policy*, *supra* note 40.

48. *See Atlas Privacy Policy*, *supra* note 45.

preferences for profit.[49] Furthermore, within the past year Facebook changed its privacy policy by "disregard[ing] its users' choice of using their in-browser 'Do Not Track' setting; any user who "clicks 'ask websites not to track me' in Safari (or any other browser) will be completely ignored by Facebook."[50] Unlike data brokering companies that have recently been reprimanded[51] for their deceitful tactics, the validity of social media sites' privacy policies and terms of use have not been challenged by the Federal Trade Commission.[52]

---

49. *Facebook Data Policy*, *supra* note 40. Because Facebook owns Instagram, the same advertising policies apply. *Instagram Privacy Policy*, *supra* note 26. Twitter has a similar policy where it sells information to itself through in-house groups like Atlas, called "third-party ad partners." *Twitter Privacy Policy*, TWITTER, https://twitter.com/privacy?lang=en [https://perma.cc/ME2Q-ZF8L] (last visited Aug. 4, 2016).

50. Violet Blue, *Facebook Turns User Tracking 'Bug' Into Data Mining 'Feature' for Advertisers*, ZDNET BLOG (June 17, 2014, 12:01 AM), http://www.zdnet.com/ article/facebook-turns-user-tracking-bug-into-data-mining-feature-for-advertisers/ [https://perma.cc/P8KU-JWU4]. However, Facebook will honor users' do-not-track settings on mobile apps like Android and iOS devices. *See id.* To do this, users must opt out by going to the Digital Advertising Alliance, an external website; however, if a user clears their browser's cookies, they must opt out again. *Id.*

51. Recently, a data mining company was at the forefront of a scandal: the FTC charged the data broker with "illegally selling payday loan applicants' financial information to a scam operation" that took over $7 million from consumers' accounts. *See* Press Release, Fed. Trade Comm'n, FTC Charges Data Brokers with Helping Scammer Take More than $7 Million from Consumers' Accounts (Aug. 12, 2015), https://www.ftc.gov/news-events/press-releases/2015/08/ftc-charges-data-brokers-helping-scammer-take-more-7-million [https://perma.cc/T2JX-3UK6]. The scammers used consumers' information they had purchased from the data broker to make unauthorized charges. *Id.* Consumers' accounts were drained and some were charged fees for insufficient funds. *Id.* This is not the first time that data brokers have been charged with facilitating the illegal taking of money from consumers. In 2014, the data broker LeapLab facilitated the theft of millions of dollars from consumer accounts by personal financial information to marketers who had no legitimate need for the information. *See* Press Release, Fed. Trade Comm'n, FTC Charges Data Broker with Facilitating the Theft of Millions of Dollars from Consumers' Accounts (Dec. 23, 2014), https://www.ftc.gov/news-events/press-releases/2014/12/ftc-charges-data-broker-facilitating-theft-millions-dollars [https://perma.cc/3RSK-CKX9]. These marketers, in turn, used such information to withdraw millions of dollars from consumers' accounts without their authorization. *Id*.

52. The Federal Trade Commission defines data brokers as "companies that collect information, including personal information about consumers, from a wide variety of sources for the purpose of reselling such information to their customers for various purposes, including verifying an individual's identity, differentiating records, marketing products, and preventing financial fraud." FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 68 (Mar. 2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacy report.pdf [https://perma.cc/9KJD-LBNH]. It is possible that the FTC has not reprimanded social media companies because the complexity of the companies' terms of use, combined with the unwavering success they have had in court when their terms of use have been challenged, may have discouraged users from bringing challenges to the Federal Trade Commission. *See infra* Section III.A.

However, merely reprimanding data brokering companies and imposing more restrictions on their ability to transmit the information of online users would not sufficiently protect consumers. Because social media users must consent to social media sites having an all-encompassing pass to their information in order to create a profile, restricting the ways data brokers share information only solves part of the problem; social media sites will still be able to profit from users' information from their own websites because they would not be restricted from selling this information.

Twitter infringes on its users' right to privacy more than any of the other social media sites that this Comment examines because of its behavioral advertisement policies. Twitter's Privacy Policy states that Twitter, like Facebook and Instagram, will "keep track of how [users] interact with links across [its] Services, including [its] email notifications, third-party services, and client applications . . . to provide more relevant advertising."[53] Twitter uses two kinds of first-party cookies—session cookies and persistent cookies—"to better understand how [users] interact with [their] Services, [and] to monitor aggregate usage by [their] users."[54] While Twitter's policy is similar to that of Facebook and Instagram because retailers and other third-party service providers may collect cookies, its privacy policies differ slightly: Twitter allows third-parties to collect a user's IP address and mobile device ID, websites visited, or a "cryptographic hash of a common account identifier (such as an email address) to help [Twitter] measure and tailor ads."[55] Essentially, Twitter will allow third-party advertisers to identify individual users, which is something that not even Facebook allows.[56] Thus, the sponsored

53. *Twitter Privacy Policy*, *supra* note 49.

54. While a session cookie keeps track of users' activity over a short period of time, persistent cookies aggregate this data over a users' entire use of the social media site. *Id.*

55. *Id.*

56. *Facebook Data Policy*, *supra* note 40. Another way retailers and other companies can track consumers' online activities is through their IP address. Anything that is connected to the Internet will have an internal protocol (IP) address, which enables correct data to be delivered whenever users go online; for example, IP addresses ensure that emails reach the correct recipient, and allow users to connect to the right web page when typing a URL into the search bar. Davey Winder, *Can You Really Be Traced from Your IP Address?*, ALPHR (Mar. 28, 2011), http://www.alphr.com/features/366349/can-you-really-be-traced-from-your-ip-address [https://perma.cc/7UYL-H6FU]. The IP address system "allows computers to both recognize one another and transfer data over the Internet," which is why public IP addresses leave an online footprint. Raymond Placid & Judy Wynekoop, *Tracking Down Anonymous Internet Abusers: Who is John Doe?*, 85 FLA. BAR. J. 38 (2011). In theory, it should be easy to track down the IP address of an online user because the address should be stored in IP address logs; however, this task can prove more difficult if IP address logs are periodically purged.

advertisements that users will see when using the social media site will be directed specifically towards them.

In addition to the first-party cookies used by Instagram, Facebook and Twitter, technological advances have created a type of "super cookie" or "Flash cookie" found in Adobe Flash apps.[57] Flash cookies track consumers like first-party cookies, but "can rebuild a user's information profile even after the user has erased cookie history."[58] With the power to track consumers' every click while on social media and beyond, social media sites and other apps that use super cookies can combine the information they acquire through a users' activity on social media sites with public records, and obtain enough data to create a profile for each user.[59] This information is invaluable to a retailer because it will "enable a business to develop a broad picture about a consumer, such as identifying that the individual owns a house, runs marathons, eats healthy food, has a premium bank card, and is good in financial health."[60] This information, collected without users' knowledge or consent, provides retailers with the ability to charge social media users higher prices for the same products it sells to other users for less, simply because retailers know that certain users have the means to pay more.

57. Companies that have expanded to do business online must "better leverage the social media forum" and better target new consumers that would be interested in their products. Heather Traeger & Kris Easter, *Use of Social Media in Private Fund Offerings: Perks, Perils, and Privacy*, 13 J. BUS. & SEC. L. 143, 147 (2007). Essentially, companies have begun to "follow" their customers and potential new customers in hopes of better marketing their products and services. *Id.*

58. *Id.* Flash cookies are often embedded in web pages and are always stored outside of the browser's control: "[w]eb browsers do not directly allow users to view or delete the cookies stored by a Flash app, users are not notified when such cookies are set, and these cookies never expire." Seth Schoen, *New Cookie Technologies: Harder to See and Remove, Widely Used to Track You*, ELEC. FRONTIER FOUND. (Sept. 14, 2009), https://www.eff.org/deeplinks/2009/09/new-cookie-technologies-harder-see-and-remove-wide [https://perma.cc/KX7N-TAWD]. Thus, when users clear their cookies, Flash cookies allow a website to "respawn" the information stored from the deleted cookies circumventing traditional HTTP cookie policies. *Id.* This technology allows companies that have expanded to do business online to "better leverage the social media forum" and better target new consumers that would be interested in their products. Traeger & Easter, *supra* note 57. Essentially, companies have begun to "follow" their customers and potential new customers in hopes of better marketing their products and services. *Id.*

59. Traeger & Easter, *supra* note 57.

60. *Id.*

2. The Effect of Cookies: Retailers Are Empowered to Adjust Product Prices in Relation to Different Consumers, Allowing them to Maximize Profits with Dynamic Pricing

Dynamic Pricing uses consumers' "electronic footprint[s]"—their record of previous purchases, their addresses, and maybe the other sites they have visited to determine just how much they are willing to pay for a product or service.[61] Those consumers who can afford to pay more based on their footprint, do, while more price-sensitive consumers receive the same product or service for less.[62]

First-party cookies on social media enable retailers to sort information explicitly posted by social media users as well as other information, like usernames and email addresses, at minimal cost.[63] Consumers provide retailers with this information "whenever they make a credit card purchase . . . use free e-mail services, surf [the Internet] for information[,] or engage in social media."[64] In 2000, the concept of dynamic pricing caught the attention of many consumers when they realized that Amazon had charged customers different prices for the same DVDs.[65] Amazon claimed that it had engaged in "random price testing" but consumers were infuriated because the bookseller was treating consumers unequally.[66]

Consumers' frustrations are warranted because retailers can use this tracking technology to accurately target an individual social media user's

61. Paul Krugman, *Reckonings; What Price Fairness?*, N.Y. TIMES (Oct. 4, 2000), http://www.nytimes.com/2000/10/04/opinion/reckonings-what-price-fairness.html.

62. *Id.*

63. *See* Robert M. Weiss & Ajay K. Mehortra, *Online Dynamic Pricing: Efficiency, Equity and the Future of E-Commerce*, 6 VA. J.L. & TECH. 11, 11 (2001) (discussing the use of dynamic pricing and its impact on consumers and e-commerce).

64. Akiva A. Miller, *What Do We Worry About When We Worry About Price Discrimination? The Law and Ethics of Using Personal Information for Pricing*, 19 J. TECH. L. & POL'Y 43, 91 (2014).

65. *See* Michael J. Martinez, *Amazon Error May End 'Dynamic Pricing,'* ABC NEWS (Sept. 29, 2000), http://abcnews.go.com/Technology/story?id=119399&page=1 [https://perma.cc/N68P-ZV3C] (discussing consumers' reactions after they realized that Amazon was charging different consumers different prices for the same products).

66. *See id.* Amazon and other companies are reluctant to discuss information regarding their e-commerce practices because of the negative publicity associated with differential pricing. Adam Tanner, *Different Customers, Different Prices, Thanks to Big Data*, FORBES (Apr. 14, 2014), http://www.forbes.com/sites/adamtanner/2014/03/26/different-customers-different-prices-thanks-to-big-data/#4fae9940f31c [https://perma.cc/YN7K-G7LH]. However, in a 2012 study conducted by researchers in Spain, results showed that of the 200 online stores surveyed, Amazon, Staples, and Steam varied prices to consumers based on geographic location by as much as 166%. *Id.*

preferences and ability to pay based on their online activity.[67] While economist Paul Krugman describes dynamic pricing as "a new version of an old practice," online price discrimination is different than haggling at flea markets or shopping for a car at a dealership.[68] Unlike a flea market, where bartering and price discrimination is a common practice, online consumers are at a disadvantage because they may not realize that price differences exist.[69] Retailers may charge online users more than others for the same product based on the Internet user's prior search history or purchase history.[70] In one study, a retail photography website charged users more for the same cameras and equipment depending on whether they had previously visited comparison sites.[71] Another study from 2014 revealed that retailers do in fact show users "different prices and a different set of results, even for identical searches" depending on the type of device they are using and their search history.[72] Travel sites showed the biggest price inconsistencies, quoting some consumers hundreds of dollars more for the same hotel, simply because of the web service they were using.[73] Search engines like Orbitz, Expedia and Hotels.com "steered" Mac users to more expensive hotels than PC users.[74] In addition to travel sites, Home Depot has discriminated against users on mobile browsers by directing them toward more expensive products.[75] Amongst the users searching for products on their mobile browsers, the study further revealed that Home Depot price discriminated against Android users, charging them about 6% more on the prices of products.[76]

---

67. Anita Ramasastry, *Websites Change Prices Based on Customers' Habits*, CNN (June 24, 2005, 3:14 PM), http://www.cnn.com/2005/LAW/06/24/ramasastry.website.prices/ [https://perma.cc/WR8D-J2UT].

68. Krugman, *supra* note 61; Ramasastry, *supra* note 67.

69. Krugman, *supra* note 61.

70. *See id.*

71. Ramasastry, *supra* note 67. In addition to charging different users different prices for the same items, businesses have begun to use users' social media data and prior search histories to "make employment decisions and assess insurance risk levels" because this information is particularly telling. *See* Traeger & Easter, *supra* note 57, at 148. One insurance company assessed the risk levels of thousands of its insurance applicants through the data they received from a data broker. *Id.*

72. *See* Kara Brandeisky, *How to Beat Online Price Discrimination*, TIME (Oct. 23, 2014), http://time.com/money/3534651/price-discrimination-travelocity-orbitz-home-depot/ [https://perma.cc/Y4V9-XYGT].

73. The biggest discrepancy involved consumers using Amazon's Mechanical Turk as their web service. *See* ANIKO HANNAK, ET AL., MEASURING PRICE DISCRIMINATION AND STEERING ON E-COMMERCE WEB SITES (2014), http://www.ccs.neu.edu/home/ancsaaa/files/imc151.pdf.

74. *Id.*

75. *See id.*

76. *See id.*

Retailers that have a presence on social media are eager to take advantage of the information they can collect to maximize their profits by charging more to consumers that are able to pay more. This is just another way retailers are exploiting consumer information purchased from social media user profile data. Retailers can use consumers' information against them because there is no law that protects the online privacy of consumers. Although tracking technologies like cookies can make a user's experience more personalized because the advertisements and suggested articles cater to their individual tastes, retailers have the potential to use this information in ways unknown to consumers.[77] Sixteen years ago, a writer from the *Washington Post* warned that the "[w]eb provides a continuous feedback loop: [t]he more the consumer buys from a website, the more the website knows about him and the weaker his bargaining position is."[78] Now, however, many retailers—even those that consumers have never heard of—have access to their information because social media is facilitating the expansion of the feedback loop.

B. How Retailers Have Further Prospered from Consumers' Use of Facebook, Instagram, and Twitter

With over a billion people around the world on Facebook alone, social media has become a major part of our society for many reasons, including keeping in touch with friends and having access to news updates.[79] When Facebook was introduced to the world in 2004, the social networking site flooded universities across the country, but soon thereafter it spread to high school students and the rest of the population—professors, public figures, parents, and companies seeking to advertise their products to a massive audience.[80]

77. *What's the Future of Privacy in a Big Data World?*, PBS NEWSHOUR (Jan. 23, 2014, 6:47 PM), http://www.pbs.org/newshour/bb/nation-jan-june14-privacy2-01-23/ [https://perma.cc/HDQ9-LUE4].

78. David Streitfeld, On the Web, Price Tags Blur, WASH. POST, Sept. 27, 2000, at A01, http://www.wright.edu/~tdung/amazon.htm [https://perma.cc/SLM4-F9AS].

79. *See Social Networking Statistics*, *supra* note 12; Ferlim McGrath, *Top 10 Reasons for Using Social Media*, GLOBAL WEB INDEX (Apr. 7, 2015), https://www.globalwebindex.net/blog/top-10-reasons-for-using-social-media (discussing the social networking motivations that prompt people to use social media).

80. *See* Andre Mouton, *Social Networks: Building Empires, Not Businesses*, USA TODAY (Apr. 1, 2013, 10:11 AM), http://www.usatoday.com/story/tech/2013/04/01/social-networks-minyanville/2041801/ [https://perma.cc/LZ6T-Y2LE] (discussing the growth and

Today, social media sites have adapted to invite businesses, brands, and people to use their social media platform.[81] Facebook has created pages "for businesses, brands, and organizations to share their stories and connect with people."[82] Similarly, Twitter allows its users, both individuals and retailers, to "start telling [their] story" through Tweets, which are expressions posted by a user in 140 characters or less that can include text, photos, or videos.[83] Twitter users can include hashtags (#) within the expressions they post, which assigns a topic to a Tweet.[84] Instagram is very similar to Twitter because it enables users to use hashtags in their posts, but unlike Twitter, Instagram primarily shares information through photos and videos posted by users.[85] Users can link the photos and videos that they post on Instagram to other social media sites, including Facebook and Twitter.[86]

Social media has significantly changed the daily routines of children and adults alike, and retailers have capitalized off of consumers' newly found habits of checking social media profiles mindlessly.[87] The average person picks up their phone more than 1,500 times in a week,[88] and before even climbing out of bed, most people have already checked their emails, texts, and social media sites like Facebook and Instagram.[89] By strategically

---

popularity of social media sites like Facebook and the way these companies monetize social interactions).

81. *See* Sarah Kessler, *The History of Advertising on Facebook*, MASHABLE (June 28, 2011) http://mashable.com/2011/06/28/facebook-advertising-infographic/#PLrbyQDD4PqW [https://perma.cc/BKQ4-HP8P] (analyzing the development of Facebook since its inception in 2004).

82. *Pages*, FACEBOOK, https://www.facebook.com/help/174987089221178 [https://perma.cc/9B4A-C9KH] (last visited Aug. 4, 2016).

83. *See Getting Started with Twitter*, TWITTER, https://support.twitter.com/articles/215585 [https://perma.cc/U7KJ-H7S4] (last visited Aug. 4, 2016).

84. Twitter users can interact with one another by "favoriting," "retweeting," and replying to the tweets of others, in addition to clicking on hashtags to see Tweets other users have posted that relate to a particular topic. *See id.*

85. *See FAQ*, INSTAGRAM, https://instagram.com/about/faq/ [https://perma.cc/7V4T-7TZC] (last visited Aug. 4, 2016).

86. Because the founders of Instagram wanted users to be able to share their photos on multiple services at once to avoid the hassle users experience when uploading a photo to different social media sites, users can share the photos they upload to Instagram on other sites, such as Flickr and Foursquare. *Id.*

87. *See* Lauren Locklear, Note, *In the World of Social Media, When Does "Private" Mean Private? A Critique of Germany's Proposed Amendments to its Federal Data Protection Act*, 44 GEO. WASH. INT'L L. REV. 749, 752 (2012) (discussing the prominence of social media even in the workforce and amongst employees of all ages).

88. Victoria Woollaston, *How Often Do You Look at Your Phone? The Average User Now Picks Up Their Device More Than 1,500 Times a Week*, DAILY MAIL (Oct. 7, 2014, 9:20 AM), http://www.dailymail.co.uk/sciencetech/article-2783677/How-YOU-look-phone-The-average-user-picks-device-1-500-times-day.html.

89. In a recent study, most smartphone users admitted to using their phones without realizing it. Some of these users logged onto Facebook and browsed without thinking. *Id.*

welcoming retailers to social media, Facebook, Instagram, and Twitter have found another way to ensure their services remain free to users.[90]

Instagram has arguably become "the most intimate [of] social media networks in the world" because it is featured on nearly every follower's phone.[91] This intimacy between users and Instagram makes the social media site a treasure trove for retailers that gain the confidence of their followers.[92] When first created in October 2010, Instagram was a social media site that focused on its "mobile-only experience" to allow users to capture "everyday moments."[93] Instagram only recently expanded to allow users to access Instagram from their desktop computer.[94] Because consumers are in possession of their cell phones nearly every waking minute of every day,[95] Instagram introduced the "Like2Buy" option in 2014.[96] If a user would like to purchase a retailer's product posted on Instagram, they can do so by clicking on the link in the retailer's biography section of their profile.[97] On their Instagram profile, retailers include a link to their website that shows

90. In the past, social media users have been concerned that social media sites would begin charging their users for their services. Nicholas Carlson, *Debunked: Why You'll Never Have to Pay for Facebook*, CNN (June 18, 2010, 3:38 PM), http://www.cnn.com/2010/TECH/social.media/06/18/no.facebook.charge/ [https://perma.cc/2XVM-TL2B]. Facebook says it will never charge users to use the site because "putting up a paywall runs counter to the company's mission to make the world more open and connected." *Id.* However, Facebook has a deep profit motive in not charging its users—it makes money by bringing together as big of an audience as possible and selling that audience's attention to advertisers willing to pay billions of dollars for it. *Id*.

91. Catalin Zorzini, *The Ultimate Guide on How to Use Instagram to Generate Sales for Your Online Shop*, ECOMMERCE PLATFORMS (Aug. 24, 2015), http://ecommerce-platforms.com/ecommerce-selling-advice/the-ultimate-guide-on-how-to-use-instagram-to-generate-sales-for-your-online-shop [https://perma.cc/G6R3-9QFW].

92. *Id.*

93. Kevin Systrom, *Introducing Your Instagram Feed on the Web*, INSTAGRAM (Feb. 5, 2013), http://blog.instagram.com/post/42363074191/instagramfeed [https://perma.cc/R2WD-G9H8].

94. *Id.*

95. A recent study showed that women spend an average of ten hours per day, and men spend an average of eight hours per day, on their cell phones. *See* K. Aleisha Fetters, *You Won't Believe How Many Hours You Spend on Your Phone Each Day*, WOMEN'S HEALTH (Sept. 2, 2014), http://www.womenshealthmag.com/life/hours-you-spend-on-your-phone [https://perma.cc/MM3C-ULYT].

96. Clare O'Connor, *Buy What You 'Like': You Can Now Shop Straight from Instagram*, FORBES (Aug. 28, 2014, 9:21 AM), http://www.forbes.com/sites/clareoconnor/2014/08/28/buy-what-you-like-you-can-now-shop-straight-from-instagram/#1906591534d6 [https://perma.cc/WWE5-3Q8P].

97. *Id.*

all of the photos the retailer has uploaded to its Instagram account.[98] By clicking on the link, users will see a display of all the items for sale; by clicking on the item they want, the user will be directed to the retailer's website to purchase the item.[99]

More recently, Facebook and Twitter have also welcomed retailers to their sites by introducing similar options to buy products directly from their websites. Twitter has made it possible for users to make "In-Tweet" purchases by including a "Buy" button within the Tweets where products are available for purchase.[100] On Facebook, retailers have been encouraged to create pages for their businesses on the social media site.[101] Facebook recently announced that it will allow businesses to create shops within their Facebook pages—providing retailers with direct access to over a billion potential customers, likely the largest platform in the world.[102] Like Instagram and Twitter, this allows retailers and brands that have a social media page on Facebook to sell products directly to Facebook users without ever leaving the site.[103]

Just as social media has continued to grab a foothold in society, the nature of advertising has shifted to a more significant focus on digital marketing.[104] In 2014 alone, retailers and other businesses spent over $50

98. *See id.*

99. Nordstrom was the first retailer that introduced the Like2Buy option, eliminating the hassle that users would have to undergo in order to find a product featured on a retailer's social media page. *Id.*

100. *In-Tweet Purchases on Twitter*, TWITTER, https://support.twitter.com/articles/20171947 [https://perma.cc/K5Y7-4Y46] (last visited Aug. 4, 2016).

101. *See* Alex Kantrowitz, *Facebook Takes Big Step Forward on Commerce, Builds Shops Into the Pages*, BUZZFEED NEWS (July 15, 2015, 1:36 PM), http://www.buzzfeed.com/alexkantrowitz/facebook-takes-big-step-forward-on-commerce-builds-shops-int#.sh0VJQR56b [https://perma.cc/B2HH-G4YS] (discussing Facebook's intention to have users not only socialize on the site, but also shop without ever leaving Facebook).

102. Facebook seems committed to developing its online commerce; it introduced a "Buy" button in 2014 that made it possible for users to purchase a product directly from the business. *Testing a New Way for People to Discover and Buy Products on Facebook*, FACEBOOK, https://www.facebook.com/business/news/Discover-and-Buy-Products-on-Facebook-Test [https://perma.cc/UY9R-NYRZ] (July 17, 2014). Because "Buy buttons" are still relatively new, only about 9% of Facebook users had expressed interest in them in 2015, totaling 140 million users. Victor Luckerson, *Here's Why Buy Buttons Are Invading the Internet*, TIME (Oct. 16, 2015), http://time.com/4075560/buy-button-facebook-youtube-pinterest/ [https://perma.cc/A3T3-CTQQ]. However, this number represents a considerable amount of user-expressed interest, and Facebook will continue to search for ways to make shopping through its site easier for users. *See id.*

103. *Id.*

104. Many companies feel that due to the growth of social media, investing in ways to market in these platforms is no longer a choice, but a necessity to optimize revenues. *See* Jason Bowden, *The Impact of Social Media Marketing Trends on Digital Marketing*, SOC. MEDIA TODAY (Mar. 17, 2014), http://www.socialmediatoday.com/content/impact-social-media-marketing-trends-digital-marketing [https://perma.cc/AY6P-AEWS].

billion in online advertisements partly because social media companies have become increasingly profitable businesses.[105] Because the marketing industry has evolved to establish a very strong social media presence targeting social media users, the law must also evolve to protect consumers from being exploited by retailers.

III. LACK OF ADEQUATE CONSUMER PRIVACY RIGHT LAWS HAS LEFT SOCIAL MEDIA USERS EXPOSED TO ADVERTISERS' ADVANCED INFORMATION GATHERING TACTICS

Retailers can use social media to obtain social media users' personal information, because privacy laws have not substantially protected the privacy of consumers, particularly those with a presence on social media.[106]

Retailers infringe on social media users' privacy rights as they attempt "to squeeze revenue out of every Facebook status, Tweet, and Instagram post."[107] Despite the significant growth in technological advances, neither Congress nor any state legislature has passed laws that adequately protect consumers' online privacy, let alone their privacy on social media. In general, "there is a lack of regulation on the collection, commoditization, aggregation, and analysis of consumer data."[108] Without updated privacy

105. *See Total US Ad Spending to See Largest Increase Since 2004: Mobile Advertising Leads Growth; Will Surpass Radio, Magazines, and Newspapers This Year*, EMARKETER (July 2, 2014), http://www.emarketer.com/Article/Total-US-Ad-Spending-See-Largest-Increase-Since-2004/1010982 [https://perma.cc/GS5K-HTPH] (discussing search engines' and social media companies' past revenue increases and predicting that companies like Google and Facebook will be receiving 15% of the $200 billion media advertising market by the end of 2016).

106. With an intention to show people "how much [information] they are putting out there," an undergraduate student at Harvard recently made one of Facebook's privacy flaws apparent. *See* Trishna Thadani, *Harvard Student Loses Facebook Internship After Highlighting Privacy Flaw*, USA TODAY (Aug. 13, 2015, 8:52 PM), http://www.usatoday.com/story/tech/2015/08/13/harvard-aran-khanna-facebook/31647295/ [https://perma.cc/QLB2-R5ZL]. The student created an app that used the location information that Facebook Messenger would send in each message. *Id.* Using Facebook Messenger's location information in his newly created app, the student was able to obtain a "Facebook friend's weekly schedule . . . [and] could do this with anyone he messaged—even if they weren't friends on Facebook." *Id.*

107. *See* Hilary Milnes, *How Retailers Hack Instagram to Drive Sales*, BUS. INSIDER (Mar. 18, 2015), http://digiday.com/brands/four-retailers-tackling-shoppable-instagram/ [https://perma.cc/T8TQ-69J9].

108. Peter Segrist, *How the Rise of Big Data and Predictive Analytics Are Changing the Attorney's Duty of Competence*, 16 N.C. J.L. & TECH. 527, 531 (2015).

laws, users are left vulnerable to the tactics of retailers attempting to capitalize on the information they have obtained.[109]

A. Courts have Weighed Privacy Concerns Against Social Media Users

Thus far, courts have accepted that "despite the weaknesses and challenges of online contracts . . . as long as users are provided with an adequate opportunity to review the terms and manifest their assent," then the online social media contract that they agree to by clicking a box is enforceable.[110] As a result, social media users consensually relinquish their personal data and activity on social media sites. Social media sites then take their users' information and sell it to retailers. To date, the few courts that have heard claims of online privacy breaches have not ruled in favor of consumers.

1. In re DoubleClick Privacy Litigation[111]

The Southern District of New York was one of the first courts to publish an opinion that addressed consumers' online privacy concerns as a result of digital tracking.[112] A group of Internet users filed suit against a prominent ad-servicing company, DoubleClick, because it had collected personally identifiable information from them through cookies.[113] DoubleClick collected the names, email addresses, home and business addresses, telephone numbers,

---

109. *Id.*

110. Jared S. Livingston, *Invasion Contracts: The Privacy Implications of Terms of Use Agreements in the Online Social Media Setting*, 21 ALB. L.J. SCI. & TECH. 591, 591 (2011); *see also* Susan E. Gindin, *Nobody Reads Your Privacy Policy or Online Contract?: Lessons Learned and Questions Raised by the FTC's Action Against Sears*, 8 NW. J. TECH. & INTELL. PROP. 1, 13–14 (2009) (explaining the repercussions of clicking "I agree" on terms of service contracts that are standard adhesion contracts).

111. *In re* DoubleClick, Inc. Privacy Litig., 154 F. Supp. 2d 497 (S.D.N.Y. 2001).

112. *In re DoubleClick* has become one of the most influential cases regarding consumers' online privacy rights and the prerogative of multinational companies to track consumers' every move while online. *See id.*; Jason A. Kotzker, *The Great Cookie Caper: Internet Privacy and Target Marketing at Home and Abroad*, 15 ST. THOMAS L. REV. 727, 737 (2003) (explaining that even after "the Electronic Privacy Information Center ("EPIC") filed a complaint with the FTC alleging DoubleClick has continued to engage in 'unfair and deceptive trade practices by tracking the online activities of Internet users,'" the FTC concluded that DoubleClick had not engaged in unfair or deceptive trade practices).

113. *In re DoubleClick*, 154 F. Supp. 2d at 503. At the time that the complaint was filed in 2000, DoubleClick had already tracked enough information from the use of cookies on Internet users' computers until it had more than 100 million data profiles. *See* Rubinstein et al., *supra* note 18 (citing Heather Green, *Privacy: Outrage on the Web*, BUS. WK. 38, 38 (Feb. 1, 2000)). Privacy concerns regarding the use of cookies for advertising are not new, yet since the late 1990s, Congress has not acted to protect the online privacy of consumers. *Id.*

and Internet searches of millions of users.[114] DoubleClick used this information to create targeted advertisements for these users.[115] The users sought injunctive and monetary relief under the Electronic Communications Privacy Act, Federal Wiretap Act, Computer Fraud and Abuse Act, and state law, but the court rejected their requests.[116] The court granted DoubleClick's motion to dismiss because the Internet users failed to plead a violation of any of the three federal statutes under which they brought suit and could not provide evidence of their economic damages.[117] The court reasoned that because DoubleClick (1) "never used or disclosed consumer's PII [personally identifiable information] for purposes other than those disclosed in its privacy policy," and (2) allowed users to opt out of being tracked, the company's practice of tracking users' online activity and information did not actually harm the plaintiffs.[118]

Although DoubleClick allowed its users to opt out of tracking at the time the users filed their case, very few people knew what cookies were, how they worked, and that they could remove cookies from their computers.[119] As a result, the vast majority of Internet users were still susceptible to the seemingly unconscionable practices of DoubleClick. *In re DoubleClick* became an early precedent that facilitated the pervasive tracking behavior that retailers and social media sites continue to use today.

2. In re Facebook Privacy Litigation[120]

In this case, a group of Facebook users sued Facebook for breach of contract, violation of California's Unfair Competition Law (UCL), and

114. *In re DoubleClick*, 154 F. Supp. 2d at 503.
115. *Id.*
116. *Id.* at 503, 514–20.
117. *Id.* at 523, 526.
118. The FTC also made this finding after having investigated DoubleClick's engagements to determine whether it used unfair or deceptive practices when collecting users' information. *Id.* at 506.
119. Cookies were invented by a twenty-four-year-old programmer named Lou Montuilli in 1994. John Schwartz, *Giving the Web a Memory Cost Its Users Privacy*, N.Y. TIMES (Sept. 4, 2001), http://www.nytimes.com/2001/09/04/technology/04COOK.html. He was trying to invent a way to give the World Wide Web a memory, and his solution was for a "website's computer to place a small file on each visitor's machine that would track what the visitor's computer did at that site." *Id.* Once Internet users began to find out how cookies worked, it sparked concern amongst the public. *Id.* In 2001, a survey showed that 67% of Americans considered online privacy to be a big concern. *Id.*
120. *In re* Facebook Privacy Litig., 791 F. Supp. 2d 705 (N.D. Cal. 2011), *aff'd mem. sub nom.* Facebook Privacy Litig. v. Facebook, Inc., 572 F. App'x 494 (9th Cir. 2014).

violation of California's Consumer Legal Remedies Act (CLRA).[121] The court granted Facebook's motion to dismiss as to all three claims.[122]

The users claimed that Facebook breached its Terms of Service contract because Facebook knowingly transmitted their personal information to third-party advertisers without their consent.[123] At the time, Facebook's advertising policies prevented the social media site from "revealing any user's 'true identity' or specific information to advertisers."[124] Facebook's advertising policies, along with its data policy, comprised the Terms of Service contract between Facebook and its users whenever they created of a Facebook profile.[125]

Facebook transmitted users' information to third parties when users clicked on an advertisement posted on Facebook.[126] Upon clicking on a Facebook advertisement, Facebook would send the third-party advertiser a "Referrer Header," which contained information like the specific web address that the user was looking at prior to clicking on the advertisement.[127] Additional

121. *See id.*; CAL. BUS. & PROF. CODE § 17200 (West 2016) (protecting competitors and consumers alike from any "unlawful, unfair or fraudulent business act or practice and unfair, deceptive, or untrue or misleading advertising."); CAL. CIV. CODE § 1760 (West 2016) (protecting "consumers against unfair and deceptive business practices and provide efficient and economical procedures to secure such protection."); Am. Online, Inc. v. Superior Court, 108 Cal. Rptr. 2d 699, 710 (Ct. App. 2001) (The Consumer Legal Remedies Act is "a legislative embodiment of a desire to protect California consumers [which] furthers the strong public policy of [California]."); Cullen v. Netflix, Inc., 880 F. Supp. 2d 1017, 1025 (N.D. Cal. 2012) (holding that if a plaintiff seeks to bring a claim under the Consumer Legal Remedies Act in federal court, such state law claim must satisfy heightened pleading standards).

122. *In re Facebook*, 791 F. Supp. 2d at 714, 717.

123. *Id.* at 708–09.

124. *Id.* A user's true identity was "represented by a unique user ID number and username," but in the plaintiff's appellate brief to the Ninth Circuit, the class urged that a Facebook user's true identity also included "information tied to their identity, including details about their private lives, habits, beliefs, preferences, and interests." Allison Grande, *Facebook's Data Sharing Calls for Damages, 9th Cir. Hears*, LAW360 (Aug. 17, 2012), http://www.law360.com/articles/370712/facebook-s-data-sharing-calls-for-damages-9th-circ-hears [https://perma.cc/4GAH-65NF].

125. *In re Facebook*, 791 F. Supp. 2d at 708–09.

126. *Id.*

127. *Id.* Many have found the court's decision in *In re Facebook* unsettling because the court failed to consider the "context-based expectations" of Facebook users; particularly, the expectation that users' personal information would not be shared with other companies simply because they are interested in advertisements targeted to their tastes. Alec Wheatley, *Do-It-Yourself Privacy: The Need for Comprehensive Federal Privacy Legislation with a Private Right of Action*, 45 GOLDEN GATE U. L. REV. 265, 278 (2015). More unsettling is the fact that, with few exceptions, once a consumer consents to a social media company's terms of use, the company is free to use the information in virtually any manner it sees fit. Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1880 (2013).

information Facebook transmitted each time a user clicked on one of its advertisements included users' names, gender, and pictures.[128]

The Facebook users sought monetary relief, claiming that as a result of Facebook's breach of its Terms of Service contract they "suffered injury."[129] The court dismissed the plaintiffs' case for failure to state a claim because they could not prove actual damages and an unjust enrichment claim was not proper when also alleging an express contract.[130] The court, relying on *Gerlinger v. Amazon.Com, Inc.*, held that because the plaintiffs claimed that their user agreement with Facebook was a valid contract, they could not assert an unjust enrichment claim in the alternative.[131] Thus, the plaintiffs were left without a remedy for Facebook's intrusion on their personal privacy.[132]

The district court also rejected the plaintiffs' claims for relief under California's UCL and CLRA. To prevail under California's UCL, a party must first prove both injury in fact and loss of money or property as a result of the unfair competition.[133] While the plaintiffs claimed that their personally identifiable information was property, the court held otherwise because no case law supported such assertion.[134]

The court premised its rationale for denying recovery based on a California CLRA violation on the fact that no consumer transaction between Facebook users and the social media site had taken place.[135] In California,

128. *In re Facebook*, 791 F. Supp. 2d at 708–09. In some countries where anonymity is highly valued, local social networking sites have gained more traction than Facebook. MARIEKE DE MOOIJ, GLOBAL MARKETING AND ADVERTISING: UNDERSTANDING CULTURAL PARADOXES 250 (4th ed. 2014). For example, because Facebook promotes self-enhancement, the social networking site Mixi, which allows its users to disguise their true identity through the use of pseudonyms, is more popular than Facebook in Japan. *Id.*

129. *In re Facebook*, 791 F. Supp. 2d at 714.

130. *Id.* at 718.

131. *Id.* In *Gerlinger*, the plaintiff alleged that an agreement between Amazon and Borders Online violated federal and state antitrust law and the common law of unjust enrichment. Gerlinger v. Amazon.com, Inc., 311 F. Supp. 2d 838, 840 (N.D. Cal. 2004). Plaintiff pleaded that the defendants breached an express contract created when he purchased books from them; the contract was the basis for the plaintiff's standing. *Id.* at 856. As a result, the plaintiff could not plead unjust enrichment in the alternative when he was alleging an express contract. *Id.*

132. *In re Facebook*, 791 F. Supp. 2d at 708.

133. *Id.*

134. *Id.* Specifically, because "[l]ogic suggests [that] if a user's personally identifiable information is valuable to Facebook and its advertisers, then it should be valuable to the user as well." Grande, *supra* note 124.

135. *In re Facebook*, 791 F. Supp. 2d at 716–17.

the CLRA protects consumers harmed in "connection with a consumer transaction."[136] To have standing to sue under the CLRA, the plaintiff must be a "consumer," defined as "an individual who purchases or leases any goods or services for personal, family or household purposes."[137] Thus, because Facebook allowed anyone to create an account free of charge, the plaintiffs did not purchase Facebook's services; California's CLRA requires one to make a purchase to be a consumer with standing under the Act.[138] While the plaintiffs contended that they paid for Facebook's services with their privacy, the law did not support their argument.[139] The court did not consider the amount of money that Facebook made by selling its users' private information to retailers and other third parties. Yet, if the court would be willing to take such information into account, the amount that users "pay" by giving up their privacy rights would qualify them as "consumers" under California's CLRA.[140]

On appeal, the Ninth Circuit recognized that the "dissemination of [plaintiffs'] personal information" and their loss of the "sales value of that information" were sufficient allegations to "show the element of damages for their breach of contract and fraud claims."[141] The court remanded the case because the district court erroneously dismissed the plaintiffs' state law claims.[142] The Ninth Circuit finally recognized that Facebook's breach

136. *Id.* at 716 (citing Robinson v. HSBC Bank USA, 732 F. Supp. 2d 976, 987 (N.D. Cal. 2010)).

137. *Id.* at 717; *see also* Schauer v. Mandarin Gems of Cal., Inc., 23 Cal. Rptr. 3d 233, 240 (Ct. App. 2005) (holding that a claim under the Consumer Legal Remedies Act should be dismissed because the statutory definition of a consumer only includes individuals who seek or acquire, by purchase or lease, goods or services).

138. On its Help Center page, Facebook states that "it is a free site and will never require that [users] pay to use the site." *Create an Account*, FACEBOOK, https://www.facebook.com/help/345121355559712 [https://perma.cc/4RF7-JRE4] (last visited Aug. 4, 2016).

139. *See In re Facebook*, 791 F. Supp. 2d at 716.

140. In 2012, Facebook had about one billion users and its stock was worth between $30 and $40 per share, making the company worth around $100 billion and each user worth around $100 on average. Will Oremus, *Zuckerbergonomics: Are You Really Worth $100 to Facebook? Is Facebook Worth $100 to You?*, SLATE (Apr. 26, 2012, 12:36 PM), http://www.slate.com/articles/technology/technology/2012/04/facebook_ipo_how_much_money_does_the_social_network_make_off_each_user_.html [https://perma.cc/QE93-QQC3]. Currently, the law provides people with a set of rights—the rights to notice, access, and consent regarding the collection, use, and disclosure of personal data—allowing citizens to make decisions about how they would like to disclose their personal information. Solove, *supra* note 127. However, because this information is worth money to social media companies and advertisers, even if social media users freely provide this information, they should be entitled to the amount the information is worth to interested parties, as logic suggests. *See* Grande, *supra* note 124.

141. Facebook Privacy Litig. v. Facebook, Inc., 572 F. App'x 494, 496 (9th Cir. 2014), *aff'g in part, rev'g in part In re* Facebook Litigation, 791 F. Supp. 2d 705 (N.D. Cal. 2011).

142. *Id.* Prior to this decision, *In re Facebook* exemplified the fact that courts were reluctant to recognize the privacy rights of individuals on social media because users'

of contract, which stemmed from violating its own advertising policy, constituted a compensable harm to the plaintiffs.[143] However, despite this small win for social media users, the Ninth Circuit affirmed the district court's dismissal of the plaintiffs' claims under California's UCL and CLRA.[144] The Ninth Circuit affirmed Facebook's motion to dismiss the plaintiffs' claim under California's UCL because the plaintiffs failed to allege that they lost money or property.[145] The Ninth Circuit also affirmed Facebook's motion to dismiss the plaintiffs' claim under California's Unfair Competition Law because the plaintiffs failed to allege that they obtained anything from Facebook by purchase or consumer transaction.[146]

In re Facebook Privacy Litigation exemplifies the power that social media companies have to distribute users' private information to third parties without repercussion—even though that distribution may violate their own privacy policies.[147] Once retailers pay social media companies for that information, they can further exploit it by targeting individuals for particular ads and services based on their social media activity and ability to pay.[148] As social media sites and retailers continue to use the pervasive digital tracking technology to profit off of consumers on social media, it is imperative for Congress to pass a law that requires social media sites to change their terms of use. Currently, social media users do not have a remedy to keep their information from being exploited by social media sites and the retailers these sites conduct business with.

---

claims would not survive a motion to dismiss. *See In re Facebook*, 791 F. Supp. 2d at 714, 717.

143. *Facebook Privacy Litig.*, 572 F. App'x at 496.

144. *Id.*

145. *Id.* Although not an issue raised by Plaintiffs, had the defendants not provided a sufficient privacy policy, such omission could have been an "unfair or deceptive act or practice in or affecting commerce" under 15. U.S.C. § 45(a)(1); such an omission would also have subjected the defendants to California's unfair competition laws. However, as the Ninth Circuit stated, "information does not constitute property . . . [and] [p]ersonally identifiable information . . . does not have compensable value." 29 Sebastian Zimmeck, *The Information Privacy Law of Web Applications and Cloud Computing*, SANTA CLARA COMPUTER & HIGH TECH. L.J. 451, 458 (2013).

146. *Facebook Privacy Litig.*, 572 F. App'x at 496.

147. *See In re Facebook*, 791 F. Supp. 2d at 714.

148. *See id.*

3. In re iPhone Application Litigation[149]

In Northern California, a district court also weighed the privacy concerns of consumers in favor of Apple and other mobile industry defendants who shared personally identifiable information to third parties through the apps on their cell phones.[150] A group of iPhone users sued Apple, their mobile device manufacturer, and a number of other mobile industry companies because the defendants accessed or tracked their personal information after downloading certain free apps from the App Store.[151] The iPhone users recognized that Apple had recorded information like their "home and workplace locations, gender, age, zip code, terms searched . . . app ID and password for specific app accounts" when they downloaded apps.[152] Despite the fact that the users had standing to sue for such a violation of privacy, the court granted the defendants' motion to dismiss because the disclosure of the consumers' personal data and geolocation information was not sufficient to merit monetary relief.[153] The court reasoned that even if Apple had transmitted that information without the iPhone users' consent, the disclosure "did not constitute an egregious breach of social norms."[154] This case further demonstrates that courts have been reluctant at best to provide consumers with warranted relief after companies have exploited their information.

These recent court decisions have left social media users without remedy if their online privacy rights are violated. As University of Chicago Professor Omri Ben-Shahar pointed out, often times consumers' privacy rights are violated but are difficult to demonstrate because "we do not have actual victims who will say, look what happened to me and ask for some kind of legal protection."[155] However, even in cases like *In re Facebook*, where

149. *In re iPhone*, 844 F. Supp. 2d 1040 (N.D. Cal. 2012).

150. *See id.* at 1078.

151. In addition to Apple, the iPhone users sued Admob, Inc., Flurry, Inc., AdMarval, Inc., Google, Inc., and Medialets, Inc. *Id.* at 1048–49.

152. *Id.* at 1054–55.

153. *Id.* at 1077–78. Courts have also rejected similar arguments, such as the argument that a company's collection of personal information causes injury-in-fact due to "unauthorized" use. *See, e.g.*, Yunker v. Pandora Media, Inc., No. 11-CV-03113, 2013 U.S. Dist. LEXIS 42691, at *15–16 (N.D. Cal. Mar. 26, 2013); Hernandez v. Path, Inc., No. 12-CV-01515, 2012 U.S. Dist. LEXIS 151035, at *4 (N.D. Cal. Oct. 17, 2012) (citing Krottner v. Starbucks Corp., 628 F.3d 1139, 1141–43 (9th Cir. 2010)); Goodman v. HTC Am., Inc., No. C11-1793, 2012 U.S. Dist. LEXIS 88496, at *19–20 (W.D. Wash. June 26, 2012) (citing Warth v. Seldin, 422 U.S. 490, 501 (1975)); Low v. LinkedIn Corp., No. 11-CV-01468, 2011 U.S. Dist. LEXIS 130840, at *9 (N.D. Cal. Nov. 11, 2011).

154. *In re iPhone*, 844 F. Supp. 2d at 1063.

155. Audie Cornish, *Why Do We Blindly Sign Terms of Service Agreements?*, NPR: ALL THINGS CONSIDERED (Sept. 1, 2014), http://www.npr.org/2014/09/01/345044359/why-do-we-blindly-sign-terms-of-service-agreements.

there were victims whose privacy rights might have been violated, when they asked for legal protection the court denied them even nominal damages.[156]

Courts have upheld the validity of a majority of standard adhesion contracts between online service providers and consumers, yet many courts have not found users' breach of contract claims sufficient to survive a motion to dismiss when their privacy rights may have been violated.[157] In order to protect social media users, the federal legislature must create a privacy law geared toward reforming the terms of use of social media sites and allow consumers to have a choice regarding whether their information is collected and sold to retailers.

B. Legislative Attempts to Protect the Privacy of Online Consumers

Enacting stricter policies to favor Internet consumers has been a topic of legal controversy in the past, and the issue has not been resolved in favor of consumers.[158] California is the only state to have passed a law protecting the online privacy rights of consumers, but that law does not give consumers a solution to the very real problem of online personal data collection.[159] The Federal Trade Commission has made several recommendations to Congress regarding consumers' online privacy, yet

156. *In re* Facebook Litig., 791 F. Supp. 2d 705, 717 (N.D. Cal. 2011), *aff'd in part, rev'd in part sub nom.* Facebook Privacy Litig. v. Facebook, Inc., 572 F. App'x 494 (9th Cir. 2014).

157. *See* Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control Over Personal Information?*, 111 PENN. STATE L. REV. 587, 614–18 (2007) (comparing instances in which courts have upheld online adhesion contracts to those where courts have not upheld enforceability of such contracts). *See, e.g.*, Davidson & Assoc. v. Internet Gateway, 334 F. Supp. 2d 1164, 1177–78 (E.D. Mo. 2004) (holding that the online contract between the user and software company was valid because users must click on "I agree" to the terms and conditions before downloading the software). *But see* Comb v. Paypal, Inc., 218 F. Supp. 2d 1165, 1172 (N.D. Cal. 2002) (holding that the online contract between the user and Paypal was invalid because users could create a Paypal account without ever opening the document containing the terms of use or arbitration clause).

158. *See, e.g.*, *In re* Google, Inc. Cookie Placement Consumer Privacy Litig., 988 F. Supp. 2d 434, 439–40 (D. Del. 2013); *In re* DoubleClick, Inc. Privacy Litig., 154 F. Supp. 2d 497, 500 (S.D.N.Y 2001); Chance v. Ave. A, Inc., 165 F. Supp. 2d 1153, 1155 (W.D. Wash. 2001).

159. To comply with CalOPPA, operators of commercial websites must "[i]dentify the categories of personally identifiable information that the operator collects . . . about individual consumers who use or visit the commercial Web site or online service . . . and the third-party persons or entities" that they may share consumer information with. CAL. BUS. & PROF. CODE § 22575(b)(1) (West 2014).

only recently did the Commission introduce a discussion draft.[160] Thus far, state and federal legislatures have failed consumers because there is no law that adequately provides consumers with a defense mechanism against having their personal information collected and online presence tracked.

1. A Step in the Right Direction: California's Online Privacy Protection Act

California has been the leader in attempting to address its citizens' concerns regarding online privacy.[161] Other states have begun to follow suit by enacting laws related to e-Reader privacy,[162] privacy of personal information held by Internet Service Providers,[163] false and misleading statements in website privacy policies,[164] notice of monitoring of employee email communications and Internet access,[165] and privacy policies of government websites.[166] However, none of the enacted laws fully protect the rights of consumers

160. *See* discussion *infra* Section III.B.2.

161. To protect children's online privacy, California enacted the Privacy Rights for California Minors in the Digital World Act, allowing minors to remove or request and obtain removal of content posted on websites, online services, online apps, or mobile apps. CAL. BUS. & PROF. CODE §§ 22580–22582 (West 2015). The law also forbids website operators, online service providers, or any third parties to market products to minors who may not legally purchase them. *Id.* California has also enacted a law that protects library patrons' book records, which identify their borrowing information and use of library resources. CAL. GOV'T CODE § 6267 (West 2002). California has further enacted laws aimed at protecting the privacy of personal information held by nonfinancial businesses, and privacy policies of government websites. *See* CAL. CIV. CODE §§ 1798.83–1798.84 (West 2006); CAL. GOV'T CODE § 11019 (West 2014).

162. *See, e.g.*, ARIZ. REV. STAT. ANN. § 41-151.22 (2013); DEL. CODE ANN. tit. 6, § 1206C (West 2016); MO. REV. STAT. §§ 182.815, 182.817 (2014).

163. *See, e.g.*, CONN. GEN. STAT. § 42-471 (2009).

164. Nebraska prohibits "knowingly" making a false or misleading statement regarding the use of personal information in any privacy policy that is published or distributed on the Internet or otherwise. NEB. REV. STAT. § 87-302 (2016); *State Laws Related to Internet Privacy*, NAT'L CONFERENCE OF STATE LEGISLATURES (Jan. 5, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx [https://perma.cc/S7ZX-TYPQ]. Similarly, Pennsylvania includes false and misleading statements published online or distributed in its deceptive or fraudulent business practices statute. 18 PA. STAT. AND CON. STAT. ANN. § 4107(a)(10) (West 2016).

165. *See, e.g.*, COLO. REV. STAT. § 24-72-204.5 (2014); DEL. CODE ANN. tit. 19 § 705 (2013); TENN. CODE ANN. § 10-7-512 (2014).

166. These laws require government websites to establish privacy policies and procedures, or to incorporate machine-readable privacy policies into their websites. *See State Laws Related to Internet Privacy*, *supra* note 164. *See also* ARIZ. REV. STAT. ANN. §§ 41-4151, 41-4152 (2016); ARK. CODE ANN. § 25-1-114 (2016); CAL. GOV'T CODE § 11019.9 (West 2013); COLO. REV. STAT. §§ 24-72-501, 24-72-502; IOWA CODE § 22.11 (2016).

who have an online presence, let alone consumers who have a presence on social media.[167]

The most significant law that has attempted to address the privacy concerns of consumers who have an online presence is California's Online Privacy Protection Act (CalOPPA), which was amended in 2013.[168] CalOPPA covers a massive audience.[169] It requires any person or company operating a website that collects personally identifiable information from California consumers to post a privacy policy on its website stating what information it collects and with whom this information is shared; CalOPPA also requires businesses to comply with their privacy policies.[170] Because CalOPPA does not contain any enforcement provisions, the Legislature intended for it to be enforced under California's UCL, where only California's Attorney General's Office, district attorneys, and some city and county attorneys can file suit against businesses in violation of the law.[171]

In 2013, the California Legislature amended the statute to include three new provisions[172] to make websites' privacy policy disclosures and online services regarding behavioral tracking more transparent for consumers.[173] The new amendments were a "transparency proposal—not a Do Not Track

167. *See State Laws Related to Internet Privacy*, *supra* note 164. *See also* ARIZ. REV. STAT. ANN. §§ 41-4151, 41-4152 (2011); ARK. CODE ANN. § 25-1-114 (West 2016); CAL. GOV'T CODE § 11019.9 (West 2013); COLO. REV. STAT. §§ 24-72-501, 24-72-502 (West 2016); IOWA CODE ANN. § 22.11 (West 2016).

168. First introduced in 2003, the California Business and Professional Act § 22575, also known as the California Online Privacy Protection Act, was the first state law in the nation to require owners of commercial websites to post a privacy policy. *See California Online Privacy Protection Act*, COOLEY LLP (June 2004), https://cooley.com/files/ALERT-Cal_OPPA.pdf [https://perma.cc/5JTX-EGL9].

169. The Census's most recent estimate of California's population was 39,144,818 people. *Quick Facts*, UNITED STATES CENSUS BUREAU, http://www.census.gov/quickfacts/table/PST045215/06,00 [https://perma.cc/P6FY-QFEV] (last visited Aug. 4, 2016).

170. CAL. BUS. & PROF. CODE § 22575 (West 2014).

171. *California Online Privacy Protection Act*, CONSUMER FED'N OF CAL., http://consumercal.org/about-cfc/cfc-education-foundation/california-online-privacy-protection-act-caloppa-3/#sthash.C6rtPhLD.dpbs [https://perma.cc/3DEM-RT64] (last updated July 29, 2015).

172. BUS. & PROF. CODE § 22575(b)(5)–(b)(7).

173. *Id.*; Dominique Shelton, *California Adopts Do-Not-Track Disclosure Law: A.B. 370 Amends the California Online Privacy Protection Act (CalOPPA) to Require New Privacy Policy Disclosures for Websites, Online Services and Mobile Acts about Behavioral Targeting*, ALSTON & BIRD LLP: PRIVACY & DATA SEC. BLOG, (Sept. 20, 2013, 11:02 AM), http://www.alstonprivacy.com/california-adopts-do-not-track-disclosure-law-a-b-370-amends-the-california-online-privacy-protection-act-caloppa-to-require-new-privacy-policy-disclosures-for-websites-online-services-and-mobile/ [https://perma.cc/HZ7L-6FS5].

proposal."[174] CalOPPA amendments were not intended to protect consumers from the harsh reality that any personal information they provide online is being collected.[175]

a. Section 22575(b)(5)

The first amendment, Section 22575(b)(5), states that businesses and online services must disclose "how the operator responds to 'do not track'" signals, but phrases like "do not track" and "other parties" are not defined.[176] As a result, CalOPPA lacks clarity regarding what kinds of activities businesses must disclose.[177] This lack of clarity shields online businesses' websites and online service providers, because they may not be disclosing the true extent of the information they collect from consumers.

b. Section 22575(b)(6)

Section 22575(b)(6) aims to provide consumers with information regarding third-party tracking mechanisms, but the provision is "unnecessarily broad [and] does not distinguish between website analytics and behavioral advertising."[178] Facebook, Instagram and Twitter indicate in their privacy policies that the use of third-party tracking technologies is subject to the third-party's own privacy policy, not that of the social media site.[179] By not requiring third parties to describe the purposes that users' information will be used for, including not specifying whether third parties must follow a social media site's privacy policy or their own, CalOPPA's goal for transparency is ineffective because consumers still do not know what kind of information companies track.[180] Additionally, even if social media

174. Shelton, *supra* note 173; *see also* Bill Analysis, AB-370 Consumers: Internet Privacy, California Assemb. Comm. on Arts, Entm't, Sports, Tourism, and Internet Media, 2013–2014 Reg. Sess. (2013), http://www.leginfo.ca.gov/pub/13-14/bill/asm/ab_0351-0400/ab_370_cfa_20130422_105924_asm_comm.html [https://perma.cc/K8W3-YP62].

175. *See* BUS. & PROF. CODE § 22575. The Bill Analysis compares the previous law with the newly enacted amendments. Bill Analysis, *supra* note 174. The legislature described the Act's purpose as increasing "consumer awareness of the practice of online tracking by websites and online services, such as mobile apps" because of consumers' demand for data collected through web browsers. Ultimately, the purpose of CalOPPA was to make consumers aware of the business practices of certain websites, not to provide consumers with a solution in regards to how to prevent their personal information from being exploited online.

176. *See* BUS. & PROF. CODE § 22575(b)(5).

177. *See New Disclosures Required Under Cal. AB 370*, IT L. GROUP, http://www.itlawgroup.com/resources/articles/215-new-disclosures-required-under-cal-ab-370 [https://perma.cc/2BE3-Z4FR] (last visited Aug. 4, 2016).

178. *See id.*

179. *Facebook Data Policy*, *supra* note 40; *Instagram Privacy Policy*, *supra* note 26; *Twitter Privacy Policy*, *supra* note 49.

180. *See New Disclosures Required Under Cal. AB 370*, *supra* note 177.

sites embedded this information within their privacy policies, the likelihood that users would find such clauses is slim.[181] Thus, to make this information available to users in a way that is easily accessible, an ideal solution is to mandate social media sites to report the data they collect from users as well as the retailers they share this information with on a single centralized website.[182]

c. Section 22575(b)(7)

The last amendment, Section 22572(b)(7) was intended as a savings clause; one way businesses can satisfy the requirement established in Section 22572(b)(5) is by providing users with a link to opt out of the tracking conducted by the business website or online service.[183] By including this provision, the California Legislature is giving businesses the ability to withhold the information that CalOPPA is intended to provide consumers—whether an online service responds to a "do not track" signal—by providing consumers with the ability to choose not to be tracked.[184]

d. Shortcomings of California's Online Privacy Protection Act

While CalOPPA is a step in the right direction toward protecting the rights of consumers' online privacy, its ambiguity and failure to define significant terms makes its attempt to adequately address the concerns of consumers futile. However, using § 22575 of the California Business and Professions Code as a model, Congress should enact a new federal privacy bill that cures the flaws of CalOPPA. First, the new federal privacy law should resolve the disparities between the California Legislature's goal of creating a transparent relationship between online service providers and their consumers; second, the federal privacy law should cure CalOPPA's overbreadth and vagueness by defining essential terms.

As noted above, because the California Legislature allows companies to hide an option to opt out within their website without informing consumers

181. In a recent study, researchers calculated that if people were to take the time to read the privacy policies of online websites, the time spent reading these policies would equal $781 billion. Shankar Vedantam, *To Read All Those Web Privacy Policies, Just Take a Month Off Work*, NPR: ALL THINGS CONSIDERED (Apr. 19, 2012, 3:30 AM), http://www.npr.org/sections/alltechconsidered/2012/04/19/150905465/to-read-all-those-web-privacy-policies-just-take-a-month-off-work.

182. *See infra* discussion Section IV.A.2.

183. Shelton, *supra* note 173.

184. *See New Disclosures Required Under Cal. AB 370*, *supra* note 177.

about the type of information they collect, consumers cannot make a reasonably informed decision. In other words, if consumers are unaware of the personal information that companies are collecting from their online activity, it is unlikely they would feel the need to—opt out of such data collection. For a law to actually provide consumers with transparency regarding the information that companies collect from their online activity, the law must specify the exact information these companies collect.

Second, because the California Legislature failed to define CalOPPA's essential terms, the law is left open to interpretation, and companies can skirt around its requirements. Thus, to ensure compliance with a new federal privacy law that protects the online privacy rights of consumers who use social media, Congress must carefully define all terms essential to the purpose of the law. More specifically, Congress should enact a law that requires all companies that conduct business online, particularly social media sites, to provide consumers with the following information: the type of information that social media sites and other third parties collect, a list of the retailers and companies that buy users' information, and the choice to opt out of being tracked both by the social media sites and third parties.

2. The Federal Trade Commission's Attempt to Protect the Privacy of Consumers

The Federal Trade Commission has made a number of recommendations to Congress urging it to pass legislation to protect the online privacy of consumers, but Congress has not yet done so.

Prior to the development of social media, data mining companies would use cookies to collect data from Internet users.[185] Since its inception, the Federal Trade Commission has strongly urged Congress to pass new legislature to require data brokers to be transparent regarding their data collecting techniques, and accountable for the data they collect from users.[186]

---

185. *See* Rubinstein et al., *supra* note 18; Bill Palace, *Data Mining: What is Data Mining?*, ANDERSON GRADUATE SCH. MGMT. UCLA (1996), http://www.anderson.ucla.edu/faculty/jason.frand/teacher/technologies/palace/datamining [https://perma.cc/ZKQ3-VV2Q] (Data mining is "the process of analyzing data from different perspectives and summarizing it into useful information that can be used to increase revenue, cut costs, or both."). The process for data mining and social media mining is essentially the same. Data mining, which is used by hundreds of online data collection companies, gathers information about an individual who uses the Internet, while social media mining gathers this information from social media sites specifically. *Tracking the Companies that Track You Online*, NPR (Aug. 19, 2010, 11:00 AM), http://www.npr.org/templates/story/story.php?storyId=129298003.

186. *See generally* FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY (May 2014), https://www.ftc.gov/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014 [https://perma.cc/N6XW-BHZ8]

In 2012, the Federal Trade Commission released a privacy report addressing the concerns of many consumers in regards to data brokers' information collecting tactics.[187] The FTC urged Congress to pass legislation that would regulate data brokers.[188] It recommended two changes to improve transparency: (1) privacy notices should be "clearer, shorter, and more standardized to enable comprehension"; and (2) the data broker industry should be required to create a "centralized website where data brokers that compile and sell data for marketing could identify themselves to consumers and describe how they collect consumer data[,] and disclose the types of companies to which they sell the information."[189] By requiring data broker companies to provide consumers with the information data brokers have about them on a centralized website, consumers can easily access their collected information and choose to—opt out of being tracked should they wish.[190]

In 2012, the FTC began an investigation of the top nine data brokers to further understand the types of data gathering methods that data brokers use.[191] Although information " used or expected to be used for decisions about credit, employment, insurance, housing, and similar eligibility determinations" is regulated by the Fair Credit Reporting Act, this Act does not regulate data brokers' collection and sale of consumer data for marketing.[192] Because of the vast amount of information that data brokers collect and sell to other data brokers, the FTC recommends that Congress pass legislation "requiring data brokers to provide consumers access to their data, including sensitive data about them . . . and the ability to opt out of having it shared for marketing purposes."[193] Combined with the FTC's proposal to create a centralized website, these goals may be accomplished by:

(analyzing the policies and procedures of data brokers in order to recommend to Congress the most effective means of regulating such companies).

187. FED. TRADE COMM'N, *supra* note 52, at 64, 68.

188. *Id.* at 69.

189. *Id.* at 64.

190. *Id.*

191. *See* DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY, *supra* note 186, at 7.

192. The Federal Trade Commission enacted the statute in 1970, but because of its limited application, the Commission has been "active in examining the practices of data brokers outside the [Fair Credit Reporting Act]" since the late 1990s. *Id.* at i.

193. *Id.* at viii.

> (1) allow[ing] consumers access to their own information; (2) allow[ing] consumers to suppress the use of this information; (3) disclos[ing] to consumers the data brokers' source of information, so that if possible consumers can correct their information at the source; and (4) disclos[ing] any limitation of the opt-out option.[194]

The FTC's proposal to create a centralized website aimed at the transparency of data brokers is an ideal model for the transparency of the advertising techniques retailers use on social media.[195] However, because many online consumers may not actually know that a centralized website exists, a more effective means of accomplishing transparency within the realm of social media would be to create a similar webpage within social media sites themselves.

3. The White House Begins to Address the Online Privacy Concerns of Consumers

The Obama administration seems to have heeded the FTC's proposal. In February 2015, the White House introduced an administrative discussion draft of the Consumer Privacy Bill of Rights Act (CPBRA) to begin conversations with Congress, consumers, and industry leaders about a federal privacy law.[196] The law was introduced to "provide consumers with more control over their data, [and provide] companies with clearer ways to signal their responsible stewardship over data and strengthen relationships with customers," yet privacy groups advocate that the Obama administration's proposed bill falls short of its goals.[197] If passed, the proposed bill would "[establish] a national privacy law that sets the standard for protection of consumer data by U.S. businesses."[198] The discussion draft would require businesses to provide individuals with notice of their privacy policies, and allow individuals to review, correct, delete, and withdraw consent for their data's continued use.[199]

---

194. *Id.* at ix.

195. *See infra* Section III.B.

196. *See* CONSUMER PRIVACY BILL OF RIGHTS ACT OF 2015, *supra* note 16; Adam Chernichaw & Brandon Freeman, *White House Re-Introduces Consumer Bill of Rights Act*, WHITE & CASE (Apr. 8, 2015), http://www.whitecase.com/publications/article/white-house-re-introduces-consumer-privacy-bill-rights-act [https://perma.cc/62T7-FG69].

197. Emily Field, *Consumer Privacy Bill of Rights Falls Short, Groups Say*, LAW360 (Mar. 4, 2015), https://advance.lexis.com/document/?pdmfid=1000516&crid=6a6206f4-0170-476d-80f4-b31ad28925a8&pddocfullpath=%2Fshared%2Fdocument%2Flegalnews%2Furn%3AcontentItem%3A5GM1-8JX1-F65M-60RY-00000-00&pddocid=urn%3AcontentItem%3A5GM1-8JX1-F65M-60RY-00000-00&pdcontentcomponentid=122080&pdteaserkey=sr0&ecomp=_thhk&earg=sr0&prid=b99b80dd-2439-4d7c-a290-32de21da193f [https://perma.cc/NG9P-Y97L].

198. Chernichaw, *supra* note 196.

199. *See* CONSUMER PRIVACY BILL OF RIGHTS ACT OF 2015, *supra* note 16; Christine Carty, *United States: White House Issues Proposal for FTC-Regulated Data Privacy*

While the discussion draft has the potential to protect consumer privacy rights, the legislature must address various weaknesses before it can achieve that goal. The current draft of CPBRA fails to define what kinds of personal data are protected and does not guarantee that consumers will have the ability to "access and correct most sets of records kept by data brokers."[200] Similar to the weaknesses of CalOPPA, if CPBRA does not sufficiently define key terms, the proposed bill will be a shield for online businesses' websites instead of adequately protecting the privacy of consumers.[201]

In addition, like CalOPPA, enforcement of the proposed CPBRA is relatively weak. The White House has proposed self-regulation in its discussion draft of CPBRA; the discussion draft states that the control over companies' use of personal data shall be "supervised by a Privacy Review Board" approved by the FTC.[202] It is unlikely that an internal Privacy Review Board will adequately protect the privacy of consumers because the companies that obtain this information will be profiting from exploiting consumers, and will have no incentive to stop. Thus, without more guarded regulations from the FTC, companies are likely to continue tracking and sharing consumers' information even without their consent.

Another significant drawback of the current draft of the CBPRA is that it will charge violators privacy fines based on the number of days the violation persists, which completely ignores the number of individuals who have had their privacy rights violated.[203] For example, if a multibillion dollar company sold 1.5 million consumer records in one day, all of which belonged to consumers who chose not to have their information shared, the company would be charged a maximum of $35,000.[204] This seems like an "incredibly perverse result" because, despite violating millions of individuals' privacy rights, the company will be charged an insignificant amount.[205]

Protection, MONDAQ (Mar. 13, 2015), http://www.mondaq.com/unitedstates/x/381172/Data+Protection+Privacy/White+House+Issues+Proposal+for+FTCRegulated+Data+Privacy+Protection [https://perma.cc/K98J-J7X7] (providing an overview of the proposed Consumer Bill of Rights Act and its weaknesses).

200. *See* Carty, *supra* note 199.

201. *See infra* Section III.B.3.

202. CONSUMER PRIVACY BILL OF RIGHTS ACT OF 2015, *supra* note 16.

203. *Analysis of the Consumer Privacy Bill of Rights Act*, CTR. FOR DEMOCRACY & TECH., https://cdt.org/insight/analysis-of-the-consumer-privacy-bill-of-rights-act/ [https://perma.cc/PM49-2UCR] (last updated Mar. 2, 2015).

204. *See id.*

205. *Id.*

The purpose of CPBRA is to provide consumers with more control over the dissemination of their personal information, so the bill must create a way for consumers to edit their information that retailers and data brokers share, as well as have an opportunity to prevent such information from being traded as a commodity.

IV. PROPOSED LEGISLATIVE CHANGES TO PROVIDE SOCIAL MEDIA USERS WITH A REMEDY TO RETAILERS AND SOCIAL MEDIA COMPANIES EXPLOITING THEIR PERSONAL INFORMATION

All of consumers' activities on social media sites, from the commercial transactions they make, what they do, where they are, and with whom they interact with on a daily basis, are a record for retailers who purchase this information from social media sites.[206] If half of all U.S. residents with a presence on social media are concerned about their privacy[207] and a majority of consumers are worried about their online activity being tracked,[208] why has Congress not passed a federal privacy law that addresses the growing concerns of consumers on social media? Why not cater to consumers' needs and give them the right to delete links to their personal information found online?[209] Although the Obama administration has recognized consumers' growing concern regarding the collection and dissemination of their information, technology is advancing faster than the legislature

206. *See* John Henry Clippinger, *Facebook Is Betting Against Its Users*, HUFFINGTON POST (June 3, 2010, 12:00 PM), http://www.huffingtonpost.com/john-henry-clippinger/facebook-is-betting-again_b_599231.html [https://perma.cc/Q7QR-28MG] (discussing Facebook's new privacy policy and its authority to track users while online generally, even if not using Facebook).

207. Nearly half of the group surveyed described themselves as "very concerned" with their privacy on social media. Mathew Ingram, *Half of Those with Social Networking Profiles Are Worried About Privacy*, GIGAOM (July 14, 2010, 5:15 PM), http://gigaom.com/2010/07/14/half-of-those-with-social-networking-profiles-are-worried-about-privacy/.

208. *See* Ronald Brownstein, *Americans Know They've Already Lost Their Privacy*, ATLANTIC (June 13, 2013), http://www.theatlantic.com/business/archive/2013/06/americans-know-theyve-already-lost-their-privacy/425433/ [https://perma.cc/FAX2-YKAM] (discussing the "ongoing communication revolution" that has left many consumers concerned about their privacy); Katy Backman, *Study: NSA Scandal Is Still Setting Off Privacy Alarm Bells Among Consumers*, ADWEEK (Aug. 13. 2013, 5:35 PM), http://www.adweek.com/news/technology/study-nsa-scandal-still-setting-privacy-alarm-bells-among-consumers-151835 [https://perma.cc/6NK7-WZBF] ("Now that consumers know the NSA spooks are reviewing their every click, online privacy has become a much bigger concern.").

209. A recent survey showed that nine out of ten voters in the United States want the right to delete links to personal information that has been collected, unbeknownst to them, by online websites, including social media. *Public Opinion on Privacy*, ELEC. PRIVACY INFO. CTR., https://www.epic.org/privacy/survey/ [https://perma.cc/K9D8-8N6Z] (last visited Aug. 4, 2016). These voters would support a law that allows Internet users to ask search companies, like Google, to remove links to certain personal information. *Id*.

can keep up with.[210] Because of our very complicated legislative structure requiring any bill to "go through substantive and financial committees in each chamber, floor debate and amendment, often a conference committee between chambers, executive amendments and possibly a veto, and then veto override procedures by the legislature," no law is quickly passed.[211] Thus, it may not be possible for the legislature to more quickly respond to technological advances infringing on consumers' rights without potentially amending our legislative structure.[212]

A. Addressing Privacy Concerns by Making Changes on Social Media

With the widespread use of social media, hardly anyone takes the time to read through the countless pages of privacy policies of any service, let alone each privacy policy of every social network they have created an account on.[213] As a result, consumers blindly click on the "I agree" terms and conditions box before actually reading any online service's lengthy contract.[214]

> [T]his plays into the fiction that by clicking 'I agree' on terms and conditions before creating a social media profile or any other online service, users have 'informed consent' and fully understand that social media sites will be collecting [their] private information and sell[ing] that information to retailers who then send users targeted ads.[215]

By clicking on the "I agree" button to create any social media account, all users are agreeing to have their information and activity tracked, which is

210. The FTC, White House, FCC, GSA, and DoD amongst others recognize "the importance of user control and the commercial value of trust and privacy [more] than many financial service and social media companies." Clippinger, *supra* note 206.

211. Sean J. Kealy, *Technology & Legislative Drafting in the United States*, B.U. SCH. OF L. (Mar. 1, 2015), http://sites.bu.edu/dome/2015/03/01/technology-legislative-drafting-in-the-united-states/ [https://perma.cc/NHS9-HCNX].

212. *Id.*

213. Cornish, *supra* note 155.

214. To demonstrate that online service agreements are too lengthy and a waste of time to actually read, University of Chicago Professor Omri Ben-Shahar printed out the fifty-five-page contract that users must agree to in order to use iTunes. *Id.* He mentioned that "it looked like a 30-feet long monster of eight-point font [and] [s]o to display its enormity, [he] hung it from the roof of the building of the University of Chicago Library." *Id.*

215. *See id.*

an invasion of any users' privacy.[216] However, this fiction should not allow social media sites to track users' information and activity and sell it to retailers.

Because many courts have continued to deny consumers the right to recover even though their privacy rights had been violated, to protect online users' information from websites that encourage users to create an online account, the federal legislature must enact a privacy law geared toward reforming the terms of use of social media sites.[217] By forcing businesses to change their privacy policies, the legislature will empower consumers to protect their privacy while online because they will have the right to choose whether businesses may collect and sell their information to retailers.

1. Goals of the Federal Privacy Law

An ideal privacy law catered to protecting consumers on social media would accomplish three goals: (1) informing users of the information social media sites are collecting; (2) showing users who receives their information; and (3) allowing users to remove their information from these sites and opt out of any personal data collection in the future.

If the federal legislature were to pass the newly introduced CPBRA, Congress would first have to make significant changes to the draft before it would adequately protect consumers' privacy rights. Because social media has significantly accelerated the sharing of users' information—a problem that has existed since the widespread use of the Internet—Congress should include a section within the proposed CPBRA that regulates the practices of social media sites and retailers. The social media section within CPBRA should require all companies that conduct business online, particularly social media sites and retailers, to change their privacy policies to give consumers with existing social media profiles the choice to opt out of being tracked and having their information shared. Additionally, for users who are new to social media and to other retailers' sites that allow consumers to create an online profile, CPBRA should give these consumers the option to opt into being tracked should they wish.

---

216. Internet users are split on whether they feel that social media sites mostly create opportunities to stay connected with their network or increase the risks of unwanted privacy disclosures. *See* Brownstein, *supra* note 208.

217. *See In re* DoubleClick, Inc. Privacy Litig., 154 F. Supp. 2d 497 (S.D.N.Y. 2011); *see also In re* iPhone Application Litig., 844 F. Supp. 2d 1040 (N.D. Cal. 2012); *In re* Facebook Privacy Litig., 791 F. Supp. 2d 705 (N.D. Cal. 2011), *aff'd mem. sub nom.* Facebook Privacy Litig. v. Facebook, Inc., 572 F. App'x 494 (9th Cir. 2014).

2. Implementing a New Federal Online Privacy Law

Similar to the Federal Trade Commission's proposal and CalOPPA, the social media section within CPBRA would aim to create transparency amongst the public, social media sites, and retailers that conduct business online with data brokers. To avoid the pitfalls of CalOPPA, the new privacy law must adequately define key terms such as "social media," "third-party sharing," and "Do Not Track signals." The law must clearly outline the changes that social media sites must make to their terms of use and privacy policies, emphasizing that social media users will control whether they would like their information and activity tracked and shared. To ensure that social media sites, retailers, and consumers can easily understand the law and to avoid the vagueness of CalOPPA, the privacy policies should follow the intent of California's Assembly Bill 242: to be written in clear and concise language that is easily understood by a majority of social media users.[218]

a. Solutions for Existing Social Media Users: Deciding Whether to Opt Out

An effective means to implement the social media regulatory section would call for the Federal Trade Commission to create and regulate a single website where all social media sites post the type of information they have collected from existing users and sold to third parties. For an existing social media user to see exactly what information each social media site collects and distributes to retailers, each social media site must have a query where users of that social media site enter their login information on the centralized FTC regulated website. However, social media users

218. California's Assembly Bill 242, which was introduced by Assembly Member Chau, states: "privacy policies should be no more than 100 words, be written in clear and concise language, be written at no greater than an eighth grade reading level." Assemb. B. 242, 2013–14 Leg., Reg. Sess. (Cal. 2013), http://www.leginfo.ca.gov/pub/13-14/bill/asm/ab_0201-0250/ab_242_bill_20130206_introduced.pdf [https://perma.cc/M2DE-ND7C]. He intended to amend CalOPPA with this language because he wanted to ensure that consumers could easily understand the types of personally identifiable information that companies would share or sell to other companies. *Id.* Because 100 words would likely not be sufficient for Congress to define essential terms, the new federal privacy law should not be limited in this respect. Additionally, because a significant number of minors have Facebook profiles, and the minimum age to create a profile is thirteen, an eighth grade reading level would be appropriate. *See How Do I Report a Child Under the Age of 13?*, FACEBOOK, https://www.facebook.com/help/157793540954833 [https://perma.cc/L7G3-DZSB] (last visited Aug. 4, 2016).

may hesitate at the thought of having their personal information be stored on a government website, which could result in opposition against CPBRA. Although the FTC would ensure that the centralized website was secure, a potential threat would result if the site's security measures were breached; because every social media user's personal information that has been tracked, shared, and sold will be featured on both the FTC's centralized website and on each social media site, an outlaw might characterize the centralized website as a treasure trove of lingering profits. Massive fines and potential lawsuits may deter some, but others may see the profit potential of using this information as worth the risk if they successfully obtain this information.

Once on the FTC's centralized website, upon submitting their social media login information, users will be taken to a page that displays their personal information that each social media site collects, alongside the list of retailers that social media sites share this information with. Social media users will then have the option of selecting what information they would like shared or removed, and what kind of activity they will allow social media sites to track. For example, if Facebook users did not want all of their activity on the social media site tracked, but would consent to retailers having access to their "Likes," they would have the opportunity to save such a preference.

In addition to the centralized website, existing social media users could also opt out or make adjustments to the information that social media sites collect and track from each social media site directly. The new law would require all social media sites to include a link on the login page titled "What We Know About You." Just as on the centralized website, once a social media user clicks the link, the social media site will prompt them to enter their login information and will take them to a page where all of the information that the social media site tracks and shares will appear. Existing social media users could edit the information that they share, select which information they would like removed, and decide whether they want the social media site to track some or all of their activity.

By creating a centralized website regulated by the FTC, the CPBRA section dedicated to social media regulation will enable users to control the dissemination of their personal information. Such a practice will provide the perfect balance between protecting consumers concerned about their privacy and allowing consumers who enjoy personalized advertisements to continue to receive such services. The legislature would be requiring transparency from social media sites while providing social media users with a remedy to protect their privacy because CPBRA would require the FTC to act on users' behalf if social media sites and retailers do not honor users' privacy requests.

b. Solutions for New Social Media Users: Deciding Whether to Opt In

The social media section within CPBRA would require social media sites to further modify their policies in regards to new social media users. New social media users will have the opportunity to opt into social media tracking and personal information sharing when creating their social media profile; opting out will no longer be the default. Instead of requiring new users to "act affirmatively in order to remove information from the stream of ordinary business," consumers could prevent any misuse or distribution of their information and activity upon creating a social media profile.[219] By allowing new users to opt into social media sites' information-gathering and sharing, should they wish, the new law would eliminate the threat that existing social media users face: "dependence on sufficient notification procedures" to inform them of the potential damage and misuse of their information.[220]

When registering for a social media profile, new users will be prompted to select what kind of information they consent to having tracked and shared with retailers and third parties. The categories of information will be identical to the information found on the FTC's centralized website, except the social media site will not yet have collected this information from new users. Unlike certain websites that have all options selected automatically, the default setting for the opt-in information list will not have any option selected. Thus, if individuals would like personalized advertisements, they will have to select such an option. Once new social media users have chosen whether or not to consent to the social media site's use of their personal data, their profile will be complete.

The concept of providing consumers with the right to opt in as a form of consent is not a novel concept.[221] In the European Union, data subjects have the right to (1) opt into the use of their personal data, (2) know who is using their personal data, and (3) know the intended use of their data.[222]

219. *See* Ryan Moshell, *. . . and Then There Was One: The Outlook for a Self-Regulatory United States Amidst a Global Trend Toward Comprehensive Data Protection*, 37 TEX. TECH L. REV. 357, 380 (2005).

220. *Id.*

221. *See* Marsha Huie, Hadley*'s Liability-Limiting and Commerce-Enhancing Principles Applied in the British Commonwealth and the U.S.A.*, 11 TEX. WESLEYAN L. REV. 649, 667 (2005) (discussing the establishment of the European Union's 1995 Data Privacy Directive that provided data subjects with the opportunity to opt into companies collecting their data, rather than having to opt out).

222. *See id.*

If the data controller's use of any consumer's personal data is not for a legitimate purpose, they have the right to protest the data controller's use of their data.[223] European Union data subjects have this remedy because unlike the United States, the European Union has enacted legislation that "grant[s] a private right of legal action to persons against data controllers who violate or allow violations of the controller's obligations."[224] Because the United States Constitution does not explicitly guarantee a right to privacy, a social media section within the Consumer Privacy Bill of Rights Act would provide all consumers with a private right of legal action against all social media sites, retailers, and businesses that misuse their personal information.[225] This law will fill the previously longstanding void in American law that has allowed social media sites and retailers alike to prosper from social media users' information and activity online.

Under another theory, the Dormant Commerce Clause, which is often the source of limiting state authority, may also support Congress's passage of a federal privacy law. The Commerce Clause vests in Congress the power to "regulate commerce with foreign nations, and among the several states, and with Indian tribes."[226] When state laws unduly burden interstate commerce, federal regulation is appropriate under the Commerce Clause.[227] Because data privacy laws impact small and large businesses alike, these laws "affect far more commerce than any obscenity statute or car dealership regulation."[228] As such, regulation under the Commerce Clause would be justified.[229]

c. Effect of Ignoring Social Media Users' Privacy Requests

If a social media user has opted to keep a social media site that she uses from sharing or tracking any of her information and the site ignores her request, she has a remedy: file a complaint with the FTC through the centralized website. For an online privacy law, like the proposed CPBRA, to have any effect on data brokers, social media sites, and retailers, the FTC must impose sanctions on companies that do not abide by social media users' privacy requests.

In the past, the FTC encouraged the self-regulation of private enterprises, but social media sites and retailers "have a diminishing motive to refrain from collecting, storing, and using more of individuals' personal information

223. *See id.*
224. *See* Council Directive 95/46, art. 100a, 1995 O.J. (L 281) 31, 51 (EC); Huie, *supra* note 221.
225. *See* Huie, *supra* note 221, at 668.
226. U.S. CONST. art. I, § 8 cl. 3.
227. *See id.*
228. Tony Glosson, *Data Privacy in Our Federalist System: Toward an Evaluative Framework for State Privacy Laws*, 67 FED. COMM. L.J. 409, 433 (2015).
229. *Id.*

as these pursuits [have] grow[n] more profitable."[230] With weak enforcement provisions such as self-regulation, any privacy law will inadequately protect its intended audience—CalOPPA is a primary example of this point. Thus, for the proposed CPBRA to succeed, the FTC must impose serious sanctions on social media sites and retailers that do not honor the privacy requests of individuals.

Once social media users know that a social media site has continued to share their information or track their activity without their consent, they must file a complaint with the FTC through the FTC's centralized website for social media sites. From there, the FTC shall impose a fine on the social media sites for each individual whose information has been shared without their consent. Unlike the current discussion draft of the CPBRA, which imposes fines for violations based on the number of days a violation occurs capping maximum fines at $35,000 per day, a more effective solution would be for the FTC to fine violators based on the number of individuals affected daily.[231] Thus, if Facebook decided to sell the information of 1.5 million users in one day despite the fact that these users withdrew their consent for such action, the social media section of CPBRA would require the FTC to fine Facebook at least $1.5 million each day until this information was removed from its own records and the records of the retailers it shared such information with.[232] A social media site could appeal this decision by providing the FTC with a written statement explaining the mistake, and by providing evidence to support that such mistake was unintentional. Once the FTC reviewed those documents, if the FTC finds that such a violation was not unintentional, the company's next remedy would be in federal court. Because social media sites and retailers are often multi-billion dollar industries, in order for this privacy bill to have a true impact, the FTC must impose significant fines on violators of CPBRA in order to make a difference.

B. More Challenges to Proposed Legislation

One of the most significant challenges to the section within the CPBRA dedicated to social media reform is not support, but rather exposure.

230. *See* M. Jos Capkovic, *Our Walls in the Information Age*, 5 CRIT. STUD. J. 1, 19 (2012) (discussing how developments in technology have created a need for stronger privacy laws).
231. *Analysis of the Consumer Privacy Bill of Rights Act*, *supra* note 203.
232. *See id.*

Because current social media users will need to opt out of having their personal information shared, if they do not know about the FTC's centralized website or where to find the opt-out section on a social media site directly, retailers will continue to profit from users' presence on social media. A possible solution to this problem is for social media sites to send all of their users a message once the privacy law has passed; before users can access their social media page, they would need to read the message that explains their "opt-out" rights. To give consumers effective notice and prevent them from scrolling through an alert, such notification can include an interactive and educational component. Social media sites could require users to type a sentence that states the information they are allowing social media sites to collect and sell, or even provide a questionnaire that requires users to type correct answers in order to successfully exit from the alert. Another potential solution to create public awareness would be to generate enough publicity about the reform to grasp the attention of a community of individuals who take considerable measures to ensure their privacy is not breached—celebrities.[233] When campaigns are supported by celebrities or people with power, they are bound to generate support, or at the very least, some talk amongst the public.[234]

One of the most threatening concerns social media users may have if CPBRA is passed is the possibility that some social media sites may begin

233. A number of celebrities take considerable measures to ensure that their private lives remain out of the public eye. Some, like Jennifer Lawrence, who have commented rather extensively and passionately about their loss of privacy on the Internet, could be ideal catalysts to generate support for stricter online privacy laws. *See* Daniel Solove, *Should Celebrities Have Privacy? A Response to Jennifer Lawrence*, LINKEDIN (Nov. 14, 2014), https://www.linkedin.com/pulse/20141117100047-2259773-should-celebrities-have-privacy-a-response-to-jennifer-lawrence [https://perma.cc/2QSV-Q4T8].

234. For example, NBCUniversal has had a long-standing commitment to its viewers and their communities in "addressing the nation's most pressing social issues" and has done so through its *The More You Know* initiative. *See The More You Know*, NBCUNIVERSAL, http://www.themoreyouknow.com/about/ [https://perma.cc/CCB4-VFZX] (last visited Aug. 4, 2016). While the campaign began in 1989 to recruit and retain teachers after the nation's shortage, it has continued throughout the years and even won nearly fifty national awards. *Id.* With hundreds of stars as spokespersons for the initiative who advocate for awareness of different issues from education, obesity, parental involvement, and diversity, it is no surprise that *The More You Know Initiative* has not only survived, but thrived in an ever evolving world. *See The More You Know: About*, NBCUNIVERSAL, http://www.themoreyou know.com/stars/ [https://perma.cc/VU3C-UNAY] (last visited Aug. 4, 2016). As the Managing Partner of one of the nation's largest public relations firm describes, "if a celebrity partnership could open a floodgate of media coverage, spike consumer interest[,] and positive impact [a] client's bottom line." *8 Tips from the Front Lines on Leveraging Celebrity for PR*, PR NEWSER (June 4, 2014, 3:58 PM) http://www.adweek.com/prnewser/8-tips-from-the-front-lines-on-leveraging-celebrity-for-pr/94068 [https://perma.cc/E22B-3KF3]. If this new privacy bill were to generate support from celebrities or even from *The More You Know Initiative*, many consumers would know about the centralized FTC website that would allow them to take charge of their online privacy.

to charge a subscription fee for usage. To be effective, CPBRA must require steep fines for any social media user's privacy violation; thus, to survive such mishap, social media sites that have significantly less users than Facebook may begin to charge consumers a subscription fee. This could cause a public outcry because social media has become a routine part of everyday life. And, to some, free social media may outweigh their right to privacy.

Moreover, because social media users willingly post information online, many may already know that the information they freely share will not be private. Because every person values privacy differently, it may be difficult to generate enough support for a new privacy law that restricts retailers' access to users' information profiles that they purchased from social media sites. While some consumers feel that the ads targeted to their needs are empowering because the ads they see while browsing social media are catered to their particular tastes, many users feel the amount of advertisements featured on social media takes away from their experience. However, by allowing retailers to benefit from dynamic pricing on advertisements to increase their revenue, as well as from the behavioral advertising that tracks users' information and activity to cater ads to their unique personalities, the amount of advertisements users see on social media will likely increase.[235]

V. CONCLUSION

Social media has exacerbated a privacy issue that has existed since the growth of the Internet. As a result, the billions of social media users who constantly Tweet, Instagram, and "Like" status updates on Facebook are providing retailers with the information these companies need to exploit users' wants by charging them differently-priced goods and services based on their ability to pay. Social media users have not had any remedy for the tracking and selling of their data because there has been no law that recognizes their right to privacy. The injustice of social media sites and retailers profiting off of the information that Internet users provide, often unknowingly, must end. Social media sites must be regulated and required to provide more favorable terms of use for consumers, allowing consumers to stop the dissemination of their information. Congress must enact a law that enables consumers to take control over their privacy rights. With the proper

235. *See* Shea Bennett, *70% of Marketers Will Increase Social Media Spend in 2015*, ADWEEK, (Jan. 12, 2015, 6:00 PM), http://www.adweek.com/socialtimes/social-marketing-2015/504357 [https://perma.cc/RZ52-5PSY].

modifications, the Consumer Privacy Bill of Rights Act will empower all consumers with an online presence to take control of their privacy rights.