Socially Private: Striking a Balance Between Social Media and Data Privacy

Adam A. Garcia[*]

ABSTRACT: For better or for worse, social media is prevalent in our technological internet-connected world. While social media users consume the services the platforms offer, the platforms in turn consume and share personal information of the user. Based on the current model, social media platforms have been scrutinized over their invasion of user privacy, particularly over what information they gather from the user and how they share that information with third parties. In a way, users have agreed to this treatment of their data, but there is arguably a line to draw. Unfortunately for users, the legal protections and remedies are unfulfilling. This piece raises the issue on how users can continue to participate in social functions online while maintaining their privacy. Self-sovereign identity—the theoretical model of providing a person with autonomous control over their information—coupled with blockchain or a distributed ledger, a technical solution with mechanisms to control how information is permissively shared, provides an opportunity to strike that balance. This solution provides users with more control over their information and may simplify legal analysis in future privacy violations. In addition, the technical solution provides tangential benefits to enhance security for the data, increase transparency over how information is shared, and ease identification of breaches.

---

[*] J.D. Candidate, The University of Iowa College of Law 2022. Thank you to everyone who helped me critique and edit this piece, especially the Iowa College of Law faculty, Writing Center, and the *Iowa Law Review* editors, who invested great time and effort to polish this. All remaining errors are my own.

I. INTRODUCTION

"[T]his is a major trust issue," claimed Mark Zuckerberg in an interview following the exposure of Facebook's entanglement with Cambridge Analytica's use of information from Facebook users.[1] Earlier, the news broke that Facebook allowed Cambridge Analytica to access Facebook users' information without their knowledge or express consent.[2] Several days after Zuckerberg's interview, the initial projection of exposed user information increased from

1. Kevin Roose & Sheera Frenkel, *Mark Zuckerberg's Reckoning: 'This Is a Major Trust Issue'*, N.Y. TIMES (Mar. 21, 2018), https://www.nytimes.com/2018/03/21/technology/mark-zuckerberg-q-and-a.html [https://perma.cc/E9WL-AL53].

2. *See* Julia Carrie Wong, *The Cambridge Analytica Scandal Changed the World - But It Didn't Change Facebook*, GUARDIAN (Mar. 18, 2019, 1:00 AM), https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook [https://perma.cc/4VXV-3A56].

50 million to 87 million users.[3] In April 2018, at subsequent congressional hearings, Congress hinted at regulating Facebook and companies with similar business models, but to date Congress has not acted.[4]

Social media platforms have grown at alarming rates,[5] and users readily sign up by providing personal information in exchange for full access.[6] Current business models for social media platforms almost categorically require users to provide information knowingly (for example, when they create an account) or unknowingly (such as, information derived from their browsing history), which allows a platform to develop a thorough understanding of any user.[7] Behind the curtain, however, social media companies share data and analytics about that information with third parties and users have little to no control over these exchanges.[8] When these platforms engage in data sharing agreements with third parties, user information is increasingly exposed to potential loss or misuse, and the monetary penalties do little to deter or remedy this situation.[9] Legislation has a noticeable gap failing to hold the platform companies accountable for their management in data privacy, and calls to arms by legislators typically come after an identified breach yet quickly lose momentum.[10]

Those who wish to rely on existing privacy rights need to navigate a spectrum of legal protection, which is also scattered and fragmented.[11] In theory, self-sovereign identity—an alternate technical model—has shown promise in a variety of online transactions and has potential to be used in social media.[12]

This Note discusses the prevalence of social media while highlighting the data transaction between the user and platform and how to mitigate issues accompanying that transaction. Part II of this Note lays the foundation for social media, including how social media is defined and how users interact with social media platforms, in order to understand the data transaction in depth. Part III discusses the current issues with protections, or lack thereof, of user information on social media platforms. Part IV proposes implementing a self-sovereign identity approach where users inherently will have more control over their information and how it is used. This Note argues

3. Nicholas Confessore, *Cambridge Analytica and Facebook: The Scandal and the Fallout So Far*, N.Y. TIMES (Apr. 4, 2018), https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html [https://perma.cc/G24G-MR9E].

4. *See id.*

5. Esteban Ortiz-Ospina, *The Rise of Social Media*, OUR WORLD IN DATA (Sept. 18, 2019), https://ourworldindata.org/rise-of-social-media [https://perma.cc/9GA4-4DEF].

6. *See infra* Section II.A.

7. *See infra* Section III.A.

8. *See infra* Section II.B.

9. *See infra* Section III.B.

10. *See infra* Section III.C.

11. *See infra* Section II.C.

12. *See infra* Part IV.

that the self-sovereign identity solution can mitigate users' legal privacy concerns because they are more cognizant of what information is shared. In addition, the solution provides auxiliary benefits, such as balancing the bargaining power between social media platforms and users; streamlining legal analysis in the context of consent and reasonable expectations of privacy in social media transactions; and clearly identifying examples of companies misusing data because of the nature of the technical implementation.

II. THE TYPICAL SOCIAL MEDIA TRANSACTION AND THE DATA IMPLICATIONS

Like . . . retweet . . . upvote . . . skip ad. These actions likely sound familiar because of the popularity of the software application or website with which they are affiliated—Facebook, Twitter, Reddit, and YouTube, respectively—and the prevalence of these social media platforms in our lives.[13] For instance, Facebook records approximately 2.6 billion active monthly users and Instagram, which is owned by Facebook,[14] has slightly over 1 billion active monthly users.[15] These platforms have grown their user base tremendously and are seemingly interwoven into daily routines. But, while these applications have their benefits, they also have hidden costs. Section II.A defines social media, provides a high-level explanation for its appeal, details how to create a social media presence, and explains the consequence of creating a profile. Section II.B elaborates on how social media platforms conduct business with other companies. Section II.C provides an overview on the current privacy protections available to consumers using social media, and Section II.D introduces an emerging technical solution that may alter the current model of consumer identity.

A. SOCIAL MEDIA: DEFINITION, SIGNING UP, AND DATA DISCLOSURE

While the term "social media" is readily recognizable and quickly associated with applications such as Instagram and Facebook, it is imperative to provide a definition instead of referencing an example to suffice for explanation.[16] In other words, simply naming a social media application does not fully explain what social media is. First, this Section defines social media. Second, this Section addresses why social media attracts a large user

13. *See* H. Tankovska, *Most Popular Social Networks Worldwide as of April 2021, Ranked by Number of Active Users*, STATISTA (June 29, 2021), https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users [https://perma.cc/YWM5-7RU5].

14. Sam Shead, *Facebook Owns the Four Most Downloaded Apps of the Decade*, BBC NEWS (Dec. 18, 2019), https://www.bbc.com/news/technology-50838013 [https://perma.cc/Q729-B4JE].

15. *See* Tankovska, *supra* note 13.

16. *See* Jonathan A. Obar & Steve Wildman, *Social Media Definition and the Governance Challenge: An Introduction to the Special Issue*, 39 TELECOMM. POL'Y 745, 745–46 (2015) (discussing how individuals may synonymize the term "social media" with examples of applications without defining the term).

population, and then concludes with an overview of the basic process for creating an account. These discussions create a comprehensive view on social media.

The definition of social media varies depending on the source, but each definition provides a foundation to develop a workable definition from common characteristics. In synthesizing these definitions, social media means an electronic platform connected to the internet that enables users to create and maintain an online profile, consume services to connect socially with other users, and create and share content.[17] This definition includes users' access to the platform from mobile devices or personal computers, and the term "content" encompasses the information users consume, create, and convey. In effect, this definition should include the typical social media platforms, such as Facebook and YouTube, but also blogs like Tumblr, posting reviews about businesses or locations such as Yelp, and collaborating or promoting personal endeavors online, such as LinkedIn.[18]

Social media users report a multitude of reasons why they use the platforms.[19] These reasons include staying in touch with family members and current friends, reconnecting with long-lost friends, connecting with other users who share similar interests, following public figures, and shopping.[20] Apart from these seemingly practical reasons, there are deeper, physiological or psychological reasons why users are seemingly glued to their screens.[21] One explanation is that social media is where users "communicate or use media to

17. *See Social Media*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/social%20omedia [https://perma.cc/QU76-XF8K] ("[A] form[] of electronic communication . . . through which users create online communities to share information, ideas, personal messages, and other content . . . ."); Kristen L. Mix, *Discovery of Social Media*, 5 FED. CTS. L. REV. 119, 120 (2011); James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137, 1142 (2009) (defining social media to emulate virtually a social network and incorporate sociology to encompass a user's desire to interact with people); Evan E. North, Note, *Facebook Isn't Your Space Anymore: Discovery of Social Networking Websites*, 58 U. KAN. L. REV. 1279, 1284 (2010) (highlighting "three primary activities[:] . . . [(1)] users create a unique online identity[; (2)] establish relationships with other users[;] and [(3)] join various communities of users who share connections"); Obar & Wildman, *supra* note 16, at 745–50 (providing common characteristics to outline what social media is).

18. *See* Mix, *supra* note 17, at 120; Grimmelmann, *supra* note 17, at 1142–44.

19. Aaron Smith, *Why Americans Use Social Media*, PEW RSCH. CTR. (Nov. 15, 2011), https://www.pewresearch.org/internet/2011/11/15/why-americans-use-social-media [https://perma.cc/6LCU-NVK9].

20. *Id.*

21. *See generally* Anita Whiting & David Williams, *Why People Use Social Media: A Uses and Gratifications Approach*, 16 QUALITATIVE MKT. RSCH. 362 (2013), https://www.emerald.com/insight/content/doi/10.1108/QMR-06-2013-0041/full/html [https://perma.cc/KJT6-QRJJ] (conducting a small study to understand why consumers use social media).

gratify needs or wants."[22] Another related explanation is addiction.[23] Users are addicted to the quick, short-term pleasure they experience when they log in to their profile and see activity on their account, or when they receive a notification on a device from a social media platform.[24] The brain associates notifications on our mobile devices from social media platforms with anticipating or experiencing a reward, resulting in "the potential . . . [for] a positive social stimulus and dopamine influx."[25] In fact, social media companies arguably exploit these behaviors to nurture a user's addiction and stay connected.[26] Lastly, social media companies aspire to grow their user base and develop marketing schemes.[27] People are social beings who crave social contact, so these platforms provide a virtually unlimited source to fulfill that craving.[28] Ultimately, the explanation for why social media platforms are appealing and have such a vast number of users is likely best understood in the murky middle: practical use, psychological and physiological, marketing, and social contact. However, while social media is easily accessible, users intentionally and unintentionally compromise appeal by disclosing information.

To fully participate in and consume a platform's services, a user must create a profile,[29] otherwise the user can interact at a superficial level and only view publicly posted content, perhaps for a limited time.[30] For example, a

---

22. *See* Zizi Papacharissi & Alan M. Rubin, *Predictors of Internet Use*, 44 J. BROAD. & ELEC. MEDIA 175, 176 (2000); Whiting & Williams, *supra* note 21 (reporting on the various types of uses, including social interaction, passing the time, entertainment, relaxation, a forum to express an opinion, or a tool to communicate).

23. *See* Trevor Haynes, *Dopamine, Smartphones & You: A Battle for Your Time*, HARV. UNIV.: SCI. IN THE NEWS (May 1, 2018), http://sitn.hms.harvard.edu/flash/2018/dopamine-smartphones-battle-time [https://perma.cc/9JN2-3YYM]. Dopamine, a chemical produced by the brain, is known to be released when people exercise or eat delicious food. *Id.* It is a chemical that is released when the brain predicts pleasure. Ananya Mandal, *Dopamine Functions*, NEWS MED. LIFE SCIS. (Apr. 9, 2019), https://www.news-medical.net/health/Dopamine-Functions.aspx [https://perma.cc/SY6G-WXKN].

24. Haynes, *supra* note 23.

25. *Id.*

26. *See* Devika Girish, *'The Social Dilemma' Review: Unplug and Run*, N.Y. TIMES (Sept. 9, 2020), https://www.nytimes.com/2020/09/09/movies/the-social-dilemma-review.html [https://perma.cc/RXJ3-UJ9X] (reviewing a documentary where Dr. Anna Lembke suggested social media companies exploit cognitive patterns).

27. *See* THE SOCIAL DILEMMA, (Exposure Labs, Argent Pictures, & The Space Program 2020) (showing a former Facebook executive in charge of user growth conducting a seminar and discussing the growth model to encourage existing users to invite friends to create a profile).

28. *See id.* (discussing how people are "social beings" and the platforms enable users to connect with other people and enjoy social interaction).

29. *See, e.g.*, President Joe Biden, FACEBOOK, https://www.facebook.com/POTUS [https://perma.cc/8P2P-76SK] (clicking on "like" or "share" is disabled until a person logs in).

30. Caroline Cakebread, *You're Note Alone, No One Reads Terms of Service Agreements*, INSIDER (Nov. 15, 2017, 6:30 AM), https://www.businessinsider.com/deloitte-study-91-percent-agree-terms-of-service-without-reading-2017-11 [https://perma.cc/H2SQ-EC5X]; *see also Twitter Privacy Policy*, TWITTER (June 18, 2020), https://twitter.com/en/privacy [https://perma.cc/TW6G-MJZH]

person browsing Instagram without an account is not able to click and expand a photo or watch a video.[31] After a short period of browsing, the platform displays a window that states "Log in to continue," which indicates the user cannot view any more content unless the person has an account.[32] Companies use these techniques to nudge people towards creating an account, and users are motivated so they can consume the content.[33]

While creating a profile, a user has to divulge several pieces of personal information and must accept the platform's terms of service. During the typical sign-up process, a user will provide information such as name, email address, birthdate, cell phone number, zip code, and sometimes gender.[34] Alternatively, some platforms allow users to create a profile by linking an existing profile from a different platform.[35] For instance, Reddit allows potential members to sign up by "continu[ing] with Google" or "continu[ing] with Apple."[36] In effect, the user in that situation is sharing data with one platform stored in another.[37] Reddit can request various types of access and seek basic profile information, which may include name, email address, and perhaps a profile picture, or a copy of information from the original account, such as photos or contacts (i.e., other users to whom the user is connected).[38]

When users create their accounts, they provide personal information, which has a few different definitions. Federally, Personally Identifiable

---

[hereinafter *Twitter Privacy Policy*] (providing under the "Basic Account Information" section that consumers do not need to create an account to view public twitter profiles or watch a video but need to create an account to submit a "tweet").

31. *See, e.g.*, John Krasinski, INSTAGRAM, https://www.instagram.com/johnkrasinski [https://perma.cc/DJ8P-RVUS] (browsing a celebrity account is restricted and a user cannot watch a video).

32. *See id.*

33. *See supra* notes 19–26 and accompanying text (providing reasons why a user is first attracted to social media and why a user continues to use a platform).

34. *See Sign Up*, TWITTER, https://twitter.com/i/flow/signup [https://perma.cc/ZBA2-ZWX4] (requiring a name, phone number, and birthdate); *Sign Up for Yelp*, YELP, https://www.yelp.com/signup [https://perma.cc/8LM2-WZ6U] (requiring name, email address, zip code, and birthdate); *Create Your Google Account*, GOOGLE, https://accounts.google.com/signup/v2/webcreateaccount?service=mail&continue=https%3A%2F%2Fmail.google.com%2Fmail%2F&flowName=GlifWebSignIn&flowEntry=SignUp [https://perma.cc/B23F-ZKLE] (requiring name and other information such as a phone number to contact in case the account is locked); *Sign Up*, TIKTOK, https://www.tiktok.com/signup [https://perma.cc/9CLA-XPET] (requiring a birthdate and a phone number or email); *Download*, SNAP INC., https://www.snapchat.com/download [https://perma.cc/Y4YE-5ALB] (requiring a phone number to begin the sign up process).

35. *See, e.g.*, YELP, *supra* note 34 (creating a profile is streamlined when a user wants to sign up and log in to an existing account).

36. *Sign Up or Log In*, REDDIT, https://www.reddit.com/reddits/login [https://perma.cc/TGY4-8QQY] (accessing Reddit features requires an account and users can log in with an existing Google or Apple account).

37. *See Manage Third-Party Apps & Services with Access to Your Account*, GOOGLE, https://support.google.com/accounts/answer/3466521?hl=en [https://perma.cc/DXB4-8DHU] (explaining how platforms interact with each other when data is shared).

38. *Id.*

Information ("PII") is defined as "information . . . used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual."[39] PII can also refer to different combinations of data elements depending on the context. PII may mean a name or a social security number, a driver's license number, or biometric data[40] standing alone or combined with another data element like an address.[41] Notably, there are varying degrees of PII, such as public or non-public PII, but information may not be considered PII until it is combined with some form that is publicly available PII.[42] To the user, these definitions may not matter; however, defining and classifying information may implicate an institution's legal obligations.[43]

Before the user completes the sign-up process, the user must also agree to the terms of service and "acknowledge" the privacy policy.[44] These terms and policies outline the definitions of the agreement, how the platform should be used, how content will be governed, and how to handle arbitration and dispute resolution.[45] After a profile is created, not only can a user consume the full array of platform services, but a user can also manage his or her online identity. For example, a user on Facebook can include religious or political beliefs;[46] Twitter users can add a short biography describing their background or affiliations.[47]

When a user consents to a platform's privacy policy, the user consents to the platform gathering more information beyond the typical user's awareness. At a high level, this information is labeled as "metadata."[48] Metadata is simply

---

39. 2 C.F.R. § 200.79 (2020).

40. COLO. REV. STAT. ANN. § 6-1-713 (West 2018) (being defined in Colorado's Consumer and Commercial Affairs).

41. N.H. REV. STAT. ANN. § 638:25(I) (2021) (being defined in the New Hampshire Criminal Code).

42. *See* 2 C.F.R. § 200.79 (outlining the category of public PII and how non-PII can become PII).

43. *See* 15 U.S.C.A. § 6801(a) (West 2020) (imposing obligations on "each *financial* institution . . . to protect the security and confidentiality of . . . *nonpublic* personal information" (emphasis added)).

44. *See Create a New Account*, FACEBOOK, https://www.facebook.com/r.php?locale=en_US [https://perma.cc/9MS9-BZUY] (clicking "Sign Up" binds the user to accepting the terms, data policy, and cookie policy); YELP, *supra* note 34 (establishing a profile requires the user to agree to the terms of service and "acknowledge" the platform's privacy policy).

45. *Terms of Service*, YELP (Dec. 13, 2019), https://terms.yelp.com/tos/en_us/20200101_en_us [https://perma.cc/LPC6-RC3B]; *see also Terms of Service*, FACEBOOK (Oct. 22, 2020), https://www.facebook.com/legal/terms/update [https://perma.cc/R6EN-DRRZ] [hereinafter *Facebook Terms of Service*]; *infra* Section III.A.

46. *See Add and Edit Your Profile Info*, FACEBOOK, https://www.facebook.com/help/101765758165199 4 [https://perma.cc/896Q-PGAD].

47. *How to Customize Your Profile*, TWITTER, https://help.twitter.com/en/managing-your-account/how-to-customize-your-profile [https://perma.cc/2ANT-KB4F].

48. *See* Linda Greene, Comment, *Mining Metadata: The Gold Standard for Authenticating Social Media Evidence in Illinois*, 68 DEPAUL L. REV. 103, 107 (2018).

data about data.[49] On social media platforms, metadata provides companies with the "how, when, and where" of a user's online activity.[50] Companies collect information about the user and what the user indirectly provides, such as what pages the user visits while on the platform, the messages a user sends, and information about other users with whom a user connects.[51] However, companies may also collect device information, such as the battery level of the device connected to the platform or what web browser is used, and even information from third parties, such as a user's activities while off the platform, like user shopping habits.[52] All of this data is then stored with the social media company. Altogether, the social benefits of joining a platform come at a price—creating a profile seems free, and all that is required is providing basic information and agreeing to the platform's terms and services. But in reality, these companies quickly have access to much more.

B. DATA CONSUMPTION: PLATFORM ENHANCEMENTS AND DATA SHARING AGREEMENTS IN THE COURSE OF BUSINESS

As a platform's user base grows, so too does the amount of data the platform processes.[53] This increase in data is purportedly important for the platform. This has led to two notable instances of data consumption: analyzing data to improve platform functionality[54] and targeted marketing.[55] In pursuit of this, platforms collaborate with third parties.

Just as platforms routinely update their software to fix bugs in the code or introduce new features,[56] platforms consume a user's information to tailor the user experience in real time and improve the platform's functionality.[57] Because there is so much content on a single platform, the companies devised methods to feed users with relevant information "and weed[] out content

---

49. *Metadata*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/metadata [https://perma.cc/RF5F-2SSF].

50. Greene, *supra* note 48, at 107.

51. *Data Policy*, FACEBOOK (Jan. 11, 2021), https://www.facebook.com/privacy/explanation [https://perma.cc/9CBB-ZFS6] [hereinafter *Data Policy*, FACEBOOK].

52. *Id.*

53. *See, e.g.*, Mazdak Hashemi, *The Infrastructure Behind Twitter: Scale*, TWITTER: INFRASTRUCTURE (Jan. 19, 2017), https://blog.twitter.com/engineering/en_us/topics/infrastructure/2017/the-infrastructure-behind-twitter-scale.html [https://perma.cc/9KSL-YUJ6] ("[Twitter] data centers are now 400% larger than the original design.").

54. *See, e.g.*, *Data Policy*, FACEBOOK, *supra* note 51 (analyzing data to "provide, personalize and improve [its] [p]roducts").

55. Patricia M. Wagner & Alaap B. Shah, *Free the Data! . . . Better Think Twice . . . . Legal Issues Regarding Data Sharing and Secondary Data Use*, 11 NAT'L L. REV. no. 139 (Feb. 4, 2019), https://www.natlawreview.com/article/free-data-better-think-twice-legal-issues-regarding-data-sharing-and-secondary-data [https://perma.cc/EJH5-XS3K].

56. *See, e.g.*, *Reddit*, APPLE STORE, https://apps.apple.com/us/app/reddit/id1064216828 [https://perma.cc/UN4U-4PXX] (listing updates which occur almost every one to three weeks).

57. *See Data Policy*, FACEBOOK, *supra* note 51.

that's deemed irrelevant or low-quality."[58] Platforms employ algorithms to detect what appeals to a particular user and promote suggestions so the user can find more content while browsing the platform.[59] Additionally, platforms can use technical information about a user's experience scaled by the vast number of users in order to improve the platform's overall functionality.[60] For instance, platforms use this information to protect against fraud and security risks, and improve the platform's performance.[61]

The abundancy and potential use of social media data has developed a market between social media companies and third parties where the social media company sells the data in exchange for a variety of services such as data analysis or to "consolidate posts . . . in a single app."[62] These third parties, or data brokers, are in the market for personal online information[63] and will "collect, manipulate, and share consumers' information."[64] Examples of such data brokers are companies like Acxiom, BeenVerified, and Spokeo.[65] These companies have the software and infrastructure to analyze large quantities of data allowing them to "develop[] [for instance] predictions of a consumer's interest by looking at purchase history and consumers with similar data sets."[66] Essentially, the data collected on social media platforms have perceptually become a commodity.[67]

Tracing this flow of data, users provide PII and metadata to a platform, and the social media company gathers and stores that information. Data brokers, on the other hand, may gather information from these social media companies or from a combination of public and private sources.[68] These two

58. Brent Barnhart, *Everything You Need to Know About Social Media Algorithms*, SPROUT SOC. (Mar. 26, 2021), https://sproutsocial.com/insights/social-media-algorithms [https://perma.cc/Y4MT-ZPE5].

59. *See About Twitter's Account Suggestions*, TWITTER, https://help.twitter.com/en/using-twitter/account-suggestions [https://perma.cc/6Z3S-PVFB] ("Twitter's account suggestions are based on algorithms that make personalized suggestions for you.").

60. *See Data Policy*, FACEBOOK, *supra* note 51.

61. *See Google Privacy Policy*, GOOGLE (Aug. 28, 2020), https://policies.google.com/privacy?hl=en#whycollect [https://perma.cc/BS8U-DZL3] [hereinafter *Google Privacy Policy*] (describing how the platform uses data to, among other things, develop new services, maintain and improve existing services, and provide personalized services).

62. *See* Dave Lee, *Facebook's Data-Sharing Deals Exposed*, BBC NEWS (Dec. 19, 2018), https://www.bbc.com/news/technology-46618582 [https://perma.cc/KLP4-FRC9] (covering how Facebook coordinates with other companies to process Facebook users' data).

63. Eugene E. Hutchinson, Note, *Keeping Your Personal Information Personal: Trouble for the Modern Consumer*, 43 HOFSTRA L. REV. 1151, 1155 (2015).

64. *Id.*

65. Gabrielle Olya, *Beware These 18 Industries and Companies Selling Your Information*, YAHOO FIN. (Sept. 4, 2020), https://finance.yahoo.com/news/beware-18-industries-companies-selling-090008192.html [https://perma.cc/R8EJ-6EUF].

66. Hutchinson, *supra* note 63, at 1155 n.36.

67. Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2056, 2056–57 (2004).

68. Olya, *supra* note 65.

entities arrange for data sharing agreements between each other to trade data and data analysis that the other party maintains in exchange for some form of compensation.[69] By providing these third parties with data, the third parties can conduct market analysis, population research, and market products more directly and efficiently.[70]

One important mechanism that allows social media platforms to engage in these business practices is the terms agreement and privacy policy to which users consent when signing up. For instance, when a user creates a Twitter profile, the user consents to Twitter's Privacy Policy.[71] In Section 3.2 of the Privacy Policy, Twitter provides how it may share personal data with third parties to assist the platform to function efficiently.[72] Twitter shares this information with Google Analytics, for example, to "help . . . understand the use of [its] services," meaning Twitter shares information to discern how users use its platform and tweak services to change the experience.[73] At the same time, Twitter "share[s] or disclose[s] non-personal data, such as . . . demographics . . . [or] inferred interests," but does not mention specifically with whom.[74] Social media platforms intake a wide variety of user data, which it can then commodify and share, in the name of facilitating social connectedness.

C. *THE LEGAL LANDSCAPE OF PRIVACY IN THE DATA SPACE*

Social media engages users in a public forum and, together with creating a profile, requires them to compromise some level of privacy. A user who wants to assert a privacy protection claim over PII consumed by social media platforms would have a difficult time citing to a particular law on point.[75] In all likelihood, the user has to navigate a variety of sources to develop an argument because privacy protection currently comes in several different forms and is not provided under a comprehensive framework.[76] Instead,

69. *See* Lee, *supra* note 62 (discussing the agreements Facebook made with other companies to integrate applications and personalize the experience while on the platform by accessing Facebook users' data).

70. Wagner & Shah, *supra* note 55.

71. *See Twitter Privacy Policy*, *supra* note 30.

72. *Id.*

73. *Id.* (outlining in Section 3.2 how Twitter engages with "Service Providers").

74. *Id.* (outlining in Section 3.5 the different types of information Twitter shares).

75. *See* Angelique Carson, *Data Privacy Laws: What You Need to Know in 2021*, OSANO (July 20, 2021), https://www.osano.com/articles/data-privacy-laws [https://perma.cc/QP9J-ZHS8] ("There is no one comprehensive federal law that governs data privacy in the United States. There's a complex patchwork of sector-specific and medium-specific laws, including laws and regulations that address telecommunications, health information, credit information, financial institutions, and marketing.").

76. Wendy Zhang, *Comprehensive Federal Privacy Law Still Pending*, 11 NAT'L L. REV. no. 137 (Jan. 22, 2020), https://www.natlawreview.com/article/comprehensive-federal-privacy-law-still-pending [https://perma.cc/9MA7-9845] ("[A]ll eyes will be watching to see whether the United States will finally pass a comprehensive federal privacy law . . . .").

existing privacy rights are rather piecemeal, dispersed throughout the Constitution, federal and state statutes, and case law. The law also does not specifically address user's information shared with a platform; any current support a user may find is promoted in doctrinal theory.[77] However, other doctrinal areas of law may imply an extension of privacy law to this online data. But these arguments may strain to gain traction because asserting a right to privacy in general is difficult due to the disagreement or lack of consensus on a definition of privacy.[78] This Section will introduce the history of privacy law, and then discuss various doctrinal law to piece together the important legal theories for social media data and the privacy theory this Note promotes for the proposed solution.

1. Current Piecemeal Right to Privacy

The law in the area of privacy started with the Constitution and has been interpreted in particular contexts as well. The constitutional right to privacy was not immediately recognized, but the right has developed, albeit to limited scenarios, through implicit readings of particular amendments. Before the Supreme Court recognized a right to privacy, Justice Brandeis advocated for a right of privacy and a "right 'to be let alone'" in a law review article in 1890.[79] He argued that the law developed in response to societal developments and that a right to privacy would naturally grow from "inventions and business methods."[80] In 1965, the Supreme Court in *Griswold* recognized that the Constitution implies, rather than expresses, a right to privacy from a combination of amendments.[81] The Constitution creates a "zone[] of privacy"[82] based on the "penumbras"[83] of protections provided in the First, Third, Fourth, Fifth, and Ninth Amendments.[84] For example, the Fourth and Fifth Amendments protect against intrusions into an individual's home and private life, thus creating one facet of a right to privacy.[85] Justice Harlan's concurrence in *Griswold* found a violation of privacy in the Fourteenth

77. *See Privacy*, LEGAL INFO. INST., https://www.law.cornell.edu/wex/Privacy [https://perma.cc/KNZ9-F7FV] (discussing the instances where the Supreme Court has recognized the right of privacy); *Right of Privacy: Access to Personal Information*, LEGAL INFO. INST., https://www.law.cornell.edu/wex/personal_Information [https://perma.cc/BDC4-LS4Q] (discussing a variety of federal privacy rights).

78. *See* Arthur Schafer, *Privacy: A Philosophical Overview*, *in* ASPECTS OF PRIVACY LAW 1, 1–20 (1980).

79. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890) (quoting THOMAS M. COOLEY, A TREATISE ON THE LAW OF TORTS, OR THE WRONGS WHICH ARISE INDEPENDENTLY OF CONTRACT 195 (John Lewis ed., Students' ed. 1907)).

80. *Id.*

81. Griswold v. Connecticut, 381 U.S. 479, 484–85 (1965).

82. *Id.* at 484.

83. *Id.*

84. *Id.* at 481–86.

85. *See* U.S. CONST. amends. IV, V; *see also Griswold*, 381 U.S. at 484–85.

Amendment claiming that the due process an individual is owed implicates a right to privacy.[86]

Furthermore, case law fills other gaps in legislation by carefully extending privacy rights to certain situations but also expressly defining where such rights do not apply. Numerous cases broaden the right of privacy in contexts where an individual is free to choose with whom to engage in sexual activity,[87] an unmarried individual has the right to buy contraceptives,[88] and an individual can access an abortion.[89] Other cases have expanded on Justice Harlan's view in *Griswold* that the Fourteenth Amendment protects a person's privacy in criminal cases where a person manifests a desire to maintain privacy[90] and society accepts that expectation as reasonable.[91] Courts have also found individuals have a right to privacy in their emails[92] and in cell-site location produced by a cell phone because the aggregated data could reveal intimate details of someone's life.[93] However, in the context of the Fourth Amendment searches and seizures, courts have outrightly limited the right to privacy and stated that, under the third-party doctrine, an individual does not have a "legitimate expectation of privacy in information he voluntarily turns over to third parties,"[94] nor does an individual have a right to financial records.[95] While privacy as a right has been recognized and seems to exist at large, in the area of social media the law has been silent.

Shifting towards privacy rights specifically related to technology, both federal and state laws have worked to respond to technological advances. Under their respective schemes, the laws aspire to protect individuals from

86. *See Griswold*, 381 U.S. at 499–502 (Harlan, J., concurring).

87. *See generally* Lawrence v. Texas, 539 U.S. 558 (2003) (extending the right of privacy to individuals who wish to engage in same sex sexual conduct).

88. *See generally* Eisenstadt v. Baird, 405 U.S. 438 (1972) (extending the right of privacy to unmarried individuals who wish to buy contraceptives).

89. *See generally* Roe v. Wade, 410 U.S. 113 (1973) (extending the right of privacy in the Fourteenth Amendment to provide sanctity for a woman to decide whether to have an abortion).

90. *See, e.g.*, Katz v. United States, 389 U.S. 347, 351 (1967).

91. Smith v. Maryland, 442 U.S. 735, 740 (1979).

92. *See* United States v. Warshak, 631 F.3d 266, 284–88 (2010) (finding that users of electronic email manifest an expectation of privacy and that the reasonableness of that expectation involves paramount Fourth Amendment considerations, which must keep with the pace of the technology, equating email to regular mail and granting it similar protective privacy rights).

93. *See generally* Carpenter v. United States, 138 S. Ct. 2206 (2018) (holding that an individual has a right to privacy under the Fourth Amendment in recording physical movements tracked through cell-site location).

94. *Id.* at 2216; *see Smith*, 442 U.S. at 743–44.

95. *See generally* Zietzke v. United States, 426 F. Supp. 3d 758 (W.D. Wash. 2019) (holding that an individual lacks privacy in bank records as they are produced in the course of business and the information is shared by the individual and used for financial analysis).

fraud or abuse of data and enable individuals to control their information.[96] At the federal level, the Federal Trade Commission ("FTC") is tasked with preventing "unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce."[97] The FTC may, under a variety of acts, execute its responsibilities and bring charges against companies for violating privacy policies or practices.[98] Other federal laws provide protection in specific contexts. The Children's Online Privacy Protection Act ("COPPA") of 1998, for example, provides parents with the tools needed to control information collected about their children when accessing websites.[99] Website operators are required to obtain parental consent prior to collecting a child's information and provide an opt-out option to prevent future collection.[100]

Notwithstanding federal protections, states supply their own legislation to fill the gaps of the federal legislations. For instance, in the context of health data, the Health Insurance Portability and Accountability Act ("HIPAA") of 1996 protects health information collected by healthcare providers.[101] But HIPAA does not extend to companies like Fitbit that collect health information but are considered more commercial and recreational entities.[102] In Illinois, the Biometric Information Privacy Act ("BIPA") of 2008 was enacted in response to the increasing use of biometrics "in the business and security screening sectors."[103] BIPA requires entities collecting biometric information to obtain consent before collecting biometric information; otherwise, the entity could face up to $5,000 per violation.[104] California also enacted the California Consumer Protection Act ("CCPA") of 2018 requiring for-profit businesses in California or businesses collecting information about a California consumer to provide consumers with "the right to be forgotten (deletion of information), the right to opt-out of the sale of their personal

96. *See* Privacy Act of 1974, 5 U.S.C. § 552(a) (2018); Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510–2523 (2018) (protecting communications delivered and stored electronically).

97. 15 U.S.C. § 45(a)(1) (2018).

98. *See generally* Privacy Act of 1974, 5 U.S.C. § 552(a) (2018) (protecting an individual's information stored by the government); Fair Credit Reporting Act, 15 U.S.C. § 1681 (regulating consumer crediting agencies to protect financial information).

99. *See* 15 U.S.C. §§ 6501–6506.

100. *See* 15 U.S.C. § 6502.

101. *See* Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, 110 Stat. 1936 (1996).

102. *See* 45 C.F.R. § 160.103 (2014) (defining "[c]overed entity" to include a "health plan . . . health care clearinghouse . . . [or a] health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.").

103. Biometric Information Privacy Act, 740 ILL. COMP. STAT. ANN. 14/5(a) (West 2020).

104. *Id.* at 14/15, 14/20.

information, and the right to know what information a business collects about them."[105]

2. Various Doctrinal Arguments for Privacy Protection

Although the preceding discussion establishes there is no established right to privacy over information shared on a social media platform, legal scholars argue that existing doctrines provide an argument or opportunity that an individual's information should be treated with privacy. The areas of property law, tort, or economics can lend support to data privacy protections. Ultimately this area of the law remains complicated because of definitional disagreement on what privacy even means.

One doctrinal argument is that privacy of information should be treated with similar protection as property, where property law entitles the individual to be the owner of the information.[106] The individual "could forbid [companies from] extracting information . . . without their consent," and giving this type of control would allow the individual to negotiate with companies for a certain price for their data and eliminate the concern for sharing the data with other entities.[107] For instance, a user signing up for Facebook could transfer property rights over name, birthdate, and email address. Before the transfer, the user can bargain for compensation from the PII and potentially include a premium for the information the user will create such as the metadata.

Another doctrinal argument is that tort law can expand to protect an individual's privacy. Currently, the Restatement (Second) of Torts identifies that "[o]ne who invades the right of privacy of another is subject to liability for the resulting harm to the interests of other."[108] This may come in the form of intrusion, appropriation of another's identity, unreasonable publicity to someone's life or placing aspects of that life in a negative light.[109] Indeed, the tort of invasion of privacy encompasses information publicly disclosed.[110] However, the tort does not necessarily cover information the user shares directly with the platform because the platform consumes the information and may share it with a third party, all without public disclosure.[111] And in a

105. Elaine F. Harwell, *What Businesses Need to Know About the California Consumer Privacy Act*, AM. BAR ASS'N (Oct. 7, 2019), https://www.americanbar.org/groups/business_law/publications/blt/2019/10/ca-consumer-privacy [https://perma.cc/2F7Q-BKLY]; *see* CAL. CIV. CODE § 1798.100–110 (West 2020).

106. Ignacio N. Cofone, *The Dynamic Effect of Information Privacy Law*, 18 MINN. J.L. SCI. & TECH. 517, 543 (2017).

107. *Id.* at 542–45.

108. RESTATEMENT (SECOND) OF TORTS § 652A(1) (AM. L. INST. 1977).

109. *Id.* § 652A(2).

110. *See, e.g.*, Taylor-Travis v. Jackson State Univ., 984 F.3d 1107, 1116–17 (5th Cir. 2021).

111. *See, e.g.*, Cain v. Redbox Automated Retail, LLC, 136 F. Supp. 3d 824, 835–37 (E.D. Mich. 2015). In *Cain*, the court held that consumers suing a movie retail business for sharing consumer information with partner organizations was covered by the organization's privacy

typical case concerning privacy issues and information *published online*, the courts focus particularly on the public disclosure of private facts.[112] For a user successfully to state her privacy was invaded because private facts were publicly disclosed, she must show there were: (1) private facts; (2) those facts were made public; and (3) the subject of the facts "would be highly offensive to a reasonable person" if made public.[113] It follows that social media users would have an especially difficult time asserting privacy over information they shared while on a given platform, like photos users publish. Additionally, one scholar suggests that tort law presents the foundation to recover from "the unwanted widespread broadcast of one's image or video recording on social media platforms."[114] This injury creates "its own tort—one that can unify the heterogeneous field of privacy lawsuits pertaining to social media accounts."[115]

A third doctrinal approach is arguing for privacy as a public good, similar to "clean air or national defense."[116] This argument advances the idea that the value of "privacy accrues to society"[117] and treating information with heightened caution ultimately benefits and shapes society.[118] In the context of information shared online, there is a balance to strike because information has both private and public attributes.[119] People may want to share news with friends and family about a pregnancy but hesitate if the privacy protections are inadequate.[120] The privacy discussion benefits from conceptualizing privacy as a joint effort instead of an "every-person-for-herself" approach.[121] Collectively, these doctrinal arguments advocate for and explain how to protect an individual's privacy, and consequently his or her data, by drawing

policy, and the consumers agreed to those terms. *See id.* But the distinction in public disclosure and sharing information lies in the public consuming the information compared to organizations collaborating with each for the privilege to access information. *See id.*

112. *See* J.R. v. Walgreens Boots All., Inc., 470 F. Supp. 3d 534, 552 (D.S.C. 2020); Grimes v. County of Cook, 455 F. Supp. 3d 630, 640 (N.D. Ill. 2020); Forsher v. Bugliosi, 608 P.2d 716, 724–26 (Cal. 1980).

113. *Grimes*, 455 F. Supp. 3d at 640 (quoting Karracker v. Rent-A-Ctr., Inc., 411 F.3d 831, 838 (7th Cir. 2005)). Some courts add an additional element which is to consider if "the matter is 'not of legitimate concern to the public.'" Martin v. Mooney, 448 F. Supp. 3d 72, 79 (D.N.H. 2020) (quoting Lovejoy v. Linehan, 20 A.2d 274, 276 (N.H. 2011)).

114. Zahra Takhshid, *Retrievable Images on Social Media Platforms: A Call for a New Privacy Tort*, 68 BUFF. L. REV. 139, 183 (2020).

115. *Id.* at 184.

116. Schwartz, *supra* note 67, at 2084.

117. *Id.* at 2087.

118. *Id.* at 2088. *See generally* Joshua A.T. Fairfield & Christoph Engel, *Privacy as a Public Good*, 65 DUKE L.J. 385 (2015) (analyzing privacy as a public good and the social costs individuals will calculate when deciding to disclose information).

119. *See* Fairfield & Engel, *supra* note 118, at 442.

120. *Id.* at 443.

121. *Id.* at 455–56.

on "rules or principles with such a long history in the law."[122] As a result, these arguments strengthen an expectation for privacy.

Lastly, arguments for privacy protection might nonetheless be unproductive, as scholars and philosophers have not successfully defined "privacy."[123] There have been numerous attempts to define privacy, such as "the right to be let alone"[124] or "claiming immunity from intrusion within a special 'zone' of action."[125] Every definition attempts to include situations or interests over which people would expect or appreciate privacy.[126] However, every proposed definition falls short because they do not, for example, "'fit' the data," or in other words, the definition is too narrow or too broad.[127] This endeavor demonstrates that "the ideal of privacy is clearly one of the fundamental values of our culture."[128] Even though there is a consensual desire for privacy, an elusive definition may interfere with asserting an expectation of privacy over a certain situation because there may not be a guarantee privacy includes that situation.[129] While there are many different definitions of "privacy," this Note approaches privacy from the perspective of "information control," or assessing the boundaries for an "individuals . . . to determine for themselves when, how, and to what extent information about them is communicated to others."[130]

III. LACK OF USER PROTECTION STEMMING FROM THE SOCIAL MEDIA BUSINESS MODEL AND CURRENT LEGISLATION

While the benefits of social media—connecting with friends and family or "following" celebrities—have enticed users to join, the current business model gives the user no choice over the use of his or her data. The current business model has two weaknesses: one on the front end, in lack of negotiation and transparency with the user, and one on the back end, with data sharing with third parties.[131] Though these weaknesses have been in the public spotlight and sparked concern, these companies have only made gradual changes.[132] Additionally, no federal law exists to hold data privacy and

122. *Doctrine*, LEGAL INFO. INST., https://www.law.cornell.edu/wex/doctrine [https://perma.cc/S4BP-4VPU].

123. Schafer, *supra* note 78, at 4.

124. *Id.* at 6 (quoting THOMAS MCINTYRE COOLEY, A TREATISE ON THE LAW OF TORTS, OR THE WRONGS WHICH ARISE INDEPENDENT OF CONTRACT (2d ed. 1888)).

125. *Id.* at 13.

126. *Id.* at 4–14.

127. *Id.* at 4.

128. *Id.* at 14.

129. *Id.* ("[Privacy] is not . . . regarded as an absolute value.").

130. *Id.* at 8 (quoting ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967)).

131. *See, e.g.*, *Twitter Terms of Service*, TWITTER (June 18, 2020), https://twitter.com/en/tos [https://perma.cc/NYD7-SJQX] [hereinafter *Twitter Terms of Service*].

132. *See, e.g.*, Emily Stewart, *Why Every Website Wants You to Accept Its Cookies*, VOX (Dec. 10, 2019, 8:00 AM), https://www.vox.com/recode/2019/12/10/18656519/what-are-cookies-website-

security practices to a higher standard.[133] Consequently, a user's information is at risk of being shared beyond what the user would like, and, once the information is shared, it has a heightened risk of exposure.[134] Summarily, a user lacks privacy protection over their information as a result of the disparate relationship between users and platforms on one hand, and inadequate legislative technical requirements and remedies on the other.

A. EXISTING USER CONSENT MODEL AND ATTEMPTS TO RECTIFY MODEL'S ISSUE

The first weakness deeply ingrained in the current social media business model is the lack of negotiations between a user and platform and lack of transparency in what information the platform will use.[135] In the course of creating a profile, the experience is undoubtedly uniform regardless of the platform: Users agree to provide a certain amount of information in exchange for access.[136] Typically, a user checks a box next to the phrase "Terms of Service" indicating acceptance.[137] The terms of service essentially lay out that a user assents to the platform's terms by using the services, including "email notifications, applications, buttons . . . ads, [and] commerce services."[138] As a result, the user has entered into a binding contract with the platform and will use the services appropriately.[139] These agreements are "described as an

---

tracking-gdpr-privacy [https://perma.cc/EAR5-FKRQ] ("The proliferation of . . . [cookies] was largely triggered by two different regulations in Europe: The General Data Protection Regulation . . . and the ePrivacy Directive . . . . After the GDPR went into effect, a lot of websites started adding cookie notifications."). For example, the increase in notifications about cookies, which "are pieces of information saved about [a user] when [the user is] online, and . . . track . . . [the user]," attempt to "promote transparency about . . . [a user's] online privacy." *Id.*

133. *See, e.g.*, Consumer Online Privacy Rights Act, S. GOE19A90, 116th Cong. § 107 (2019) (proposing legislation for covered entities to maintain "reasonable data security practices" and thus filling a gap in current security practice).

134. *See* Allison Grande, *Cybersecurity & Privacy Predictions for 2019*, LAW360 (Jan. 1, 2019, 12:03 PM), https://www.law360.com/articles/1112115/cybersecurity-privacy-predictions-for-2019 [https://perma.cc/A68X-DNEK].

135. *See Americans Conflicted About Sharing Personal Information with Companies*, PEW RSCH. CTR. (Dec. 30, 2015), https://www.pewresearch.org/fact-tank/2015/12/30/americans-conflicted-about-sharing-personal-information-with-companies [https://perma.cc/P6PQ-XYQS] (reporting that more than 90% of adults believe they "lost control over how personal information was collected and used by companies"). In the survey, Pew Research Center asked open-ended questions where users weighed the tradeoff between sharing "information versus the lure of convenience and cost savings." *Id.* In one response, a user rejoined Facebook as a platform to market and sell her book despite concerns over her information being collected when she first deleted her profile, thus showing the conflict between the benefit in using a platform compared to information a user provides. *Id.*

136. *See supra* notes 34–47 and accompanying text (discussing what information a user provides in order to gain full access to the services and functions a platform provides).

137. Cakebread, *supra* note 30 (reporting on a study revealing "that over 90% of consumers accept legal terms and conditions without reading them").

138. *Twitter Terms of Service*, *supra* note 131.

139. *See id.* ("You may use the Services only if you agree to form a binding contract with Twitter . . . . You may not do any of the following while accessing or using the Services: (i) access[

online adhesion contract" and are typically called "clickwraps" or "browsewraps"[140] because of the "terms and conditions governing use of an Internet website . . . to which a party assents simply by using the website."[141] These agreements are not static; social media platforms will occasionally update or change their terms and provide advanced notice to the users when this occurs.[142] If a user does not agree to the updated terms, the user can delete their profile and discontinue using the fullest extent of the services.[143]

Given the binding nature of the terms, users sign away essential rights and protections while simultaneously providing PII in exchange for full access to the platform. While mentioned during the sign-up process, a user also accepts the terms articulated under the platform's privacy policy, and, shrouded under paragraphs conditioning proper use, the platform's dispute provisions.[144] The privacy policy outlines what information a platform gathers about a given user: public information, such as time zone and language,[145] personal information, and what type of device is being used to access the website.[146] Along the same lines, the dispute resolution terms are consistent from platform to platform. The terms outline that, should disputes arise, the user agrees to resolve them exclusively in that state where they conduct their business, for example, in California.[147] Other terms provide arbitration clauses that outline similar conditions.[148] Courts have consistently upheld the validity of these clickwrap agreements under different circumstances, which binds users to the arbitration or dispute resolution clauses.[149] In sharpening the teeth of these terms under the Federal Arbitration Act, courts will order parties to handle their grievances provided there is a provision in the contract

---

or] tamper with . . . Twitter's computer services . . . (ii) probe, scan, or test the vulnerability of any system or network . . . .").

140. Selden v. Airbnb, Inc., No. 16-cv-00933, 2016 WL 6476934, at *4 (D.D.C. Nov. 1, 2016).

141. Kurtis A. Kemper, *Validity, Construction, and Application of Browsewrap Agreements*, 95 AM. L. REPS. 6th 57 § 2 (2014).

142. *Facebook Terms of Service*, *supra* note 45 (outlining under "Additional Provisions" how the platform updates its terms "to accurately reflect our services and practices").

143. *Id.* ("We hope that you will continue using our Products, but if you do not agree to our updated Terms . . . you can delete your account at any time.").

144. *See Twitter Terms of Service*, *supra* note 131 (outlining how a user agrees to the privacy policy, under Section 2, and agrees to resolve disputes following the provisions in Section 6).

145. *See Twitter Privacy Policy*, *supra* note 30.

146. *See id.*; *see also supra* notes 48–52 and accompanying text.

147. *See Twitter Terms of Service*, *supra* note 131; *see also Facebook Terms of Service*, *supra* note 45.

148. *See Terms of Use*, INSTAGRAM (Dec. 20, 2020), https://help.instagram.com/581066165581870 [https://perma.cc/DC4A-T88Z].

149. *See* Selden v. Airbnb Inc., No. 16-cv-00933, 2016 WL 6476934, at *5 (D.D.C. Nov. 1, 2016) (providing three circumstances where clickwrap agreements are upheld: (1) where the terms and conditions are hyperlinked "next to the only button that will allow the user to continue us[ing] the website[;]" (2) where a user is presented with hyperlinks to the terms "on subsequent visits"; and (3) where the user is presented with notice "on multiple successive webpages of the site" (citations omitted) (quoting Berkson v. Gogo LLC, 97 F. Supp. 3d 359, 400–01, (E.D.N.Y. 2015)).

requiring arbitration.[150] Consequently, users are disadvantaged if they want to file a claim because of the company's internal handling of the data or because the data was compromised and disclosed, intentionally or unintentionally, to a third party.[151] The user might have to litigate in a foreign forum or not litigate at all and stomach the issue if the privacy policy addressed the situation.[152] Altogether, this demonstrates that the user provides PII and surrenders legal protection in exchange for using the platform.

Moreover, this weakness is exacerbated by the often lengthy terms of service and privacy policy and the potential indefinite retention of information.[153] A recent study found that approximately one percent of social media users read the terms and conditions.[154] When a court evaluates the binding effect of the clickwrap agreement, the court determines whether the user had notice of the terms.[155] A court may find that the user had constructive notice of the terms and hold those terms as binding.[156] Then, the user is bound to an enormous amount of terms all without reading or understanding them.[157] Buried within these terms are clauses governing data retention. In some instances, a user may delete her account and try to remove any PII and content she shared, but the platform may retain it for an indefinite amount of time.[158] Notably, the platform's privacy policy does not govern the data retention practices of third parties, so it is possible PII may never be deleted.[159]

---

150. *See* 9 U.S.C. § 2 (2018).

151. *See* Thomas H. Koenig & Michael L. Rustad, *Fundamentally Unfair: An Empirical Analysis of Social Media Arbitration Clauses*, 65 CASE W. RSRV. L. REV. 341, 341–42 (2014) (finding that arbitration clauses produce "a deterrent effect, blocking all but a handful of social media users from filing claims").

152. *See id.* at 352 ("The cost of air travel alone would far exceed what is at stake."). In the chance the terms do not provide choice of law provisions, litigants may have the freedom to choose the forum but still face litigation costs of thousands of dollars. PAULA HANNAFORD-AGOR & NICOLE L. WATERS, ESTIMATING THE COST OF CIVIL LITIGATION 7 (2013), https://www.srln.org/system/files/attachments/CSPH_online2.pdf [https://perma.cc/2SY6-H972].

153. Tim Sandle, *Report Finds Only 1 Percent Reads 'Terms & Conditions'*, DIGIT. J. (Jan. 29, 2020), http://www.digitaljournal.com/business/report-finds-only-1-percent-reads-terms-conditions/article/566127 [https://perma.cc/CHM3-9V38]; *see Twitter Privacy Policy*, *supra* note 30 (outlining under "[d]eletion" how Twitter "keep[s] Log Data for a maximum of 18 months . . . . Keep in mind that search engines and other third parties may still retain copies of your public information . . . even after you have deleted the information from our services").

154. Sandle, *supra* note 153.

155. *See* Meyer v. Uber Techs., Inc., 868 F.3d 66, 78–79 (2d Cir. 2017).

156. *See id.* (finding constructive notice where the hyperlink to the text was "reasonably conspicuous").

157. *See* CNN Business, *Zuckerberg: Average Person Doesn't Read Full Terms of Service*, YOUTUBE (Apr. 10, 2018), https://www.youtube.com/watch?v=gulnT-wi-KE [https://perma.cc/PA2F-2Y5E].

158. *See Yelp Privacy Policy*, YELP (Dec. 13, 2019), https://terms.yelp.com/privacy/en_us/20200101_en_us/#Data-Retention-and-Account-Termination [https://perma.cc/7XP8-LZFG] ("We may . . . maintain residual copies of your personal information in our backup systems.").

159. *See Twitter Privacy Policy*, *supra* note 30 (notifying users that third parties may retain information after deleting an account).

One solution consumer advocates promote for platforms to rectify this weakness has been to simplify the terms and agreements to "improve[] readability" and enhance communication and transparency for users.[160] For instance, Twitter's terms of service and privacy policy can span over 50 pages,[161] so reducing the number of pages will hopefully motivate users to read everything. Other efforts shed light on the terms of service for a given platform, highlight the important terms, and rank how well the entire agreement conveys information to users.[162] This nutshell version of agreements enhances the level of transparency but does not solve the problem of nudging people to read the terms and conditions. Ultimately, "consumer protection law is . . . being swallowed by click-by-agree clauses."[163]

B. EXISTING DATA SHARING AGREEMENTS AND SHRUGGING OFF PUBLIC PRESSURE

The second weakness is the extent to which a user's information is shared with third parties. Data sharing is less apparent to users because they do not interact directly with third parties.[164] Efforts to curb this practice or encourage more transparency in the transaction do not address the root cause and usually offer compensation instead of rectification.[165] Because social media users do not pay the platforms in exchange for access, the platforms search for other ways to monetize their business, primarily through advertisements targeted towards consumers.[166] As previously discussed, the user's information becomes the commodity,[167] which relates to the idea that "if something is free, you're the product."[168]

---

160. *See* Abner Li, *Google Updating Terms of Service to Improve Readability, Include Chrome/OS & Drive*, 9TO5 GOOGLE (Feb. 21, 2020, 12:54 PM), https://9to5google.com/2020/02/21/google-tos-update-2020 [https://perma.cc/YU5X-B5FA].

161. *See Twitter Privacy Policy*, *supra* note 30 (a downloaded version covers 19 pages); *Twitter Terms of Service*, *supra* note 131 (a downloaded version covers 39 pages).

162. *See generally Terms of Service; Didn't Read*, TOS;DR, https://tosdr.org [https://perma.cc/NW3V-5ZZM] (rating different internet companies based on their terms of service and providing salient information on those terms).

163. David Berreby, *Click to Agree With What? No One Reads Terms of Service, Studies Confirm*, GUARDIAN (Mar. 3, 2017, 8:38 AM), https://www.theguardian.com/technology/2017/mar/03/terms-of-service-online-contracts-fine-print [https://perma.cc/EWG5-2RSB].

164. *See Twitter Privacy Policy*, *supra* note 30 (outlining in Section 3.1 of the Privacy Policy that a user can change her settings if she wishes to control information Twitter shares).

165. *See* CNBC Television, *FTC Commissioner Rohit Chopra: Facebook Settlement Doesn't Fix the Issue*, YOUTUBE (July 24, 2019), https://youtu.be/l4w3W2H3p34 [https://perma.cc/N5WX-2LEU] (interviewing FTC Commissioner Rohit Chopra, who criticized a settlement with Facebook because the settlement does not allow the FTC to investigate Facebook's business practices).

166. *See* THE SOCIAL DILEMMA, *supra* note 27 (interviewing Tim Kendall, former Facebook employee, who outlined that the business model would generate revenue through advertisements).

167. *See supra* Section II.B.

168. Soumik Roy, *Facebook: If Something is Free, 'You' are the Product*, TECH HQ (Apr. 9, 2018), https://techhq.com/2018/04/facebook-if-something-is-free-you-are-the-product [https://perma.cc/HQ42-4UEF].

Data sharing agreements enable social media platforms and data brokers to share information amongst themselves and develop a holistic profile of a given user.[169] Some data brokers have sophisticated analytical systems to investigate attributes of the world population and sell their analysis to companies to be used in marketing.[170] In turn, social media companies provide in their terms and services to what extent they share information with third parties.[171] Facebook and Google, for instance, state they do not sell information but may share it in some instances.[172] For example, Facebook's Data Policy states "[w]e don't sell any of your information to anyone, and we never will."[173] At the same time, Facebook's Data Policy also states that third parties with integrated products "can receive information about what [a user] post[s] or share[s]."[174] On the other hand, Twitter's policy states it will share information but does not outrightly prohibit selling information. For instance, Twitter's policy provides that it shares information with "ad partners and affiliates."[175] However, the policy also provides that "[a]dvertising revenue allows us to support and improve our services."[176] In any case, the business relationship between platforms and third parties aims, among other things, to improve the advertisements a user receives and the platform's services.[177] Interestingly, the data sharing market even invades the public arena; public entities have been in the business of selling personal information "to private

169. *See* Kalev Leetaru, *What Does it Mean for Social Media Platforms to "Sell" Our Data?*, FORBES (Dec. 15, 2018, 3:56 PM), https://www.forbes.com/sites/kalevleetaru/2018/12/15/what-does-it-mean-for-social-media-platforms-to-sell-our-data/?sh=2843f4172d6c [https://perma.cc/RH9J-D3P9] ("In addition to merely 'selling access' to advertisers . . . Facebook also makes data available in other ways. Demographers wishing to create maps of specific combinations of traits and interests or understand their temporal changes can use advertising campaigns to create population scale insights. Similarly, advertisers running ads that link back to their sites know that every person following that link possesses the specific traits the ad targeted.").

170. *See* Olya, *supra* note 65 (listing how Acxiom has data on "more than . . . 2.5 billion addressable consumers and more than 10,000 attributes").

171. *See, e.g.*, *Data Policy*, FACEBOOK, *supra* note 51 ("Sharing with Third-Party Partners" includes providing analytical services, reports, measurements, and subscription information).

172. *Compare Data Policy*, FACEBOOK, *supra* note 51 (explaining information may be shared with an assortment of parties, including advertisers and vendors), *with Google Privacy Policy*, *supra* note 61 (explaining how Google shares information for "external processing" which entails providing information to affiliates), *and Twitter Privacy Policy*, *supra* note 30 (sharing data to improve advertisement experience or general services).

173. *Data Policy*, FACEBOOK, *supra* note 51.

174. *Id.* ("Sharing on Facebook Products").

175. *Twitter Privacy Policy*, *supra* note 30 (disclosing the relationship under Section 2.6).

176. *Id.*

177. *Compare Data Policy*, FACEBOOK, *supra* note 51 (explaining information may be shared with advertisers to improve the advertisement experience), *with Google Privacy Policy*, supra note 61 (explaining how Google improves its services by assessing a user's information), *and Twitter Privacy Policy*, *supra* note 30 (sharing data to improve advertisement experience or general services).

investigators and other third parties."[178] Social media companies are entitled to share this information because the users "agreed" to these terms.

Additionally, a consequence of sharing data to multiple sources is that the users' information is at an increased risk of unauthorized access. When this information is in multiple locations and managed by different parties, a heightened risk that information may be accessed by an unprivileged party follows.[179] Normally, a social media platform would be the primary target of hackers to access information, but "hackers look[] for the weakest link to gain access to corporate systems."[180] Since there is a "growing prevalence of third-party hacks,"[181] third parties storing a user's information pose an additional or heightened risk that the information may be stolen.[182] The third party may not implement the same security measures as the social media platform, but users must nevertheless rely on a third party's cybersecurity controls to keep the information safe.[183] In effect, the third party becomes the "weak link" because of the possibility that the third party has less stringent security, which is a risk the user must inherently accept by virtue of the terms of service.[184]

Perhaps unsurprisingly, these agreements have attracted the ire of the public. Most notably, Facebook received more than an earful in the Cambridge Analytica scandal.[185] In that situation, from 2015 to 2016, Facebook provided Cambridge Analytica access to its platform to publish a quiz.[186] Each user who took this quiz unknowingly permitted Cambridge Analytica to access their information as well as information "from their

178. Andrew Whalen, *DMVs Across the Country Selling Your Driver's License Data for as Little as a Penny, Making Them Millions*, NEWSWEEK (Sept. 6, 2019, 4:42 PM), https://www.newsweek.com/dmv-drivers-license-data-database-integrity-department-motor-vehicles-1458141 [https://perma.cc/GD9N-UKEK].

179. *See* Allison Grande, *Cybersecurity & Privacy Predictions for 2019*, LAW360 (Jan. 1, 2019, 12:30 PM), https://www.law360.com/articles/1112115/cybersecurity-privacy-predictions-for-2019 [https://perma.cc/VE5E-5CFS].

180. *Id.*

181. *Id.*

182. *See id.*

183. *Id.* In quoting Andy Gandhi:

> But [a] company has raised its fences and locked its doors, so rather than break into that company . . . hackers are looking for an easier entry point . . . [A] law firm that represents the company may not have the same fences but may have information about an M&A transaction or a cloud provider that archives its information.

Id.

184. *See id.* ("As a result of . . . the risks that third party service providers present from a security standpoint, vendor management will continue to be an area of careful focus . . . .")

185. Alexandra Ma, *Everyone Is Talking About Cambridge Analytica, the Trump-Linked Data Firm that Harvested 50 Million Facebook Profiles – Here's What's Going On*, BUS. INSIDER: INDIA (Mar. 19, 2018, 7:52 PM), https://www.businessinsider.in/tech/everyone-is-talking-about-cambridge-analytica-the-trump-linked-data-firm-that-harvested-50-million-facebook-profiles-heres-whats-goingon/articleshow/63369055.cms [https://perma.cc/JTY2-CT8K].

186. *Id.*

friends' profiles."[187] Cambridge Analytica scavenged for information from more than 87 *million* Facebook users.[188] In the public forum, congressional leaders were quick to condemn the actions of Facebook and Cambridge Analytica, and thousands of users deleted their profiles.[189] These condemnations did little to deter Facebook. In spite of this scandal, a couple years later in 2018, a report revealed that Facebook continued to share data "with more than 150 partners" who could access a user's name and read private messages all without consent.[190]

C. ISSUES WITH ENFORCING STANDARDS

The third weakness is that federal and state legislation fails to allow users to hold social media platforms accountable for negligent data management and privacy practices, and private causes of action are few and far between. Consumers, all without a comprehensive federal regime, must rely on the FTC or state officials to bring an action.[191] Legislation that appears to be on point for data management is usually limited in scope.[192] In the off-chance that users can allege an injury, they face an uphill battle.[193] Despite calls from the public and steps taken by congressional representatives to increase regulation or accountability, social media companies have almost unchecked authority to share information with third parties and can defend against actions alleging failure to protect information.[194] This Section will first discuss litigation problems at the federal, then at the state level, and finally with common law causes of action.

At the federal level, courts typically bar private parties from litigating a social media platform's negligent privacy practices but allow the FTC to proceed with such suits.[195] Under the Federal Trade Commission Act ("FTC Act"), the FTC has authority to prosecute commercial entities engaged in

187. *Id.*

188. *Facebook Scandal 'Hit 87 Million Users'*, BBC NEWS (Apr. 4, 2018), https://www.bbc.com/news/technology-43649018 [https://perma.cc/C29C-6W6J].

189. Confessore, *supra* note 3.

190. Nat Levy, *Facebook Data-Sharing Partnership with Amazon, Microsoft and Other Tech Giants at the Center of Latest Privacy Scandal*, GEEKWIRE (Dec. 19, 2018, 9:13 AM), https://www.geekwire.com/2018/facebook-data-sharing-partnerships-amazon-microsoft-tech-giants-center-latest-privacy-scandal [https://perma.cc/863R-BHMW].

191. *See* Carlson v. Coca-Cola Co., 483 F.2d 279, 280 (9th Cir. 1973) ("The protection against unfair trade practices afforded by the [Fair Trade Commission] Act vests initial remedial power solely in the Federal Trade Commission."); N.Y. GEN. BUS. § 899-bb(c) (LexisNexis 2021).

192. *See* 740 ILCS 14/10 (West 2020) (limiting scope to biometric information).

193. *See* Perdue v. Hy-Vee, Inc., 455 F. Supp. 3d 749, 759–60 (C.D. Ill. 2020).

194. *See id.* (requiring online platforms to notify a user the platform will collect information on the user and share it with third parties; by requiring this, it is inferential that such requirement did not previously exist, at least at a federal level).

195. *See, e.g.*, Wisniewski v. Rodale, Inc., 510 F.3d 294, 308 (3rd Cir. 2007) (holding there was no implied private right of action under the FTC Act).

"unfair or deceptive acts."[196] The FTC has brought actions against entities for substandard practices related to data security and privacy.[197] For instance, the FTC successfully maintained an action against Wyndham Worldwide Corporation and other defendants for a "failure to maintain reasonable and appropriate data security for consumers' sensitive personal information."[198] Additionally, the FTC has obtained substantial settlements up to $5 billion related to deceptive privacy practices, particularly for "deceiving users about their ability to control the privacy of their personal information."[199] In the Facebook Cambridge Analytica incident mentioned earlier, the FTC imposed a civil penalty on Facebook for $5 billion (the largest to date) for abusing consumer privacy, as part of a settlement agreement.[200] However, that same year, Facebook recorded a fiscal year revenue of approximately $70.7 billion.[201] These settlements, however, are limited in that they are merely a slap on the wrist. The fines are usually a drop in the bucket of the platform's financial resources, and do not allow public officials to investigate deeper and uncover (and possibly fix) the root problems.[202] Thus, if a company is alleged to be misusing information by engaging in deceptive practices, private parties must rely on the FTC's discretion to bring an action against that company, which are often settlements. Settlement agreements may attempt to cool the public's dissatisfaction, but this only goes so far.

At the state level, some legislation is similar to the federal scheme in allowing government officials to initiate legal action.[203] In New York, the Stop Hacks and Improve Electronic Data Security Act ("SHIELD Act") was enacted in early 2020 and included data security requirements, such as conducting risk assessments, testing software systems to identify and mitigate weaknesses, and use encryption.[204] Notably, the SHIELD Act applies to any person or business that consumes personal information of a New York resident, not just a party who conducts business in New York.[205] Despite these security

196. 15 U.S.C. § 45 (2018); *see also supra* Section II.C.

197. *See* Fed. Trade Comm'n v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 607 (D.N.J. 2014).

198. *Id.*

199. *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*, FED. TRADE COMM'N (July 24, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions [https://perma.cc/5QC6-NP78].

200. Lesley Fair, *FTC's $5 Billion Facebook Settlement: Record-Breaking and History-Making*, FED. TRADE COMM'N (July 24, 2019, 8:52 AM), https://www.ftc.gov/news-events/blogs/business-blog/2019/07/ftcs-5-billion-facebook-settlement-record-breaking-history [https://perma.cc/MT9G-J5PT].

201. *Facebook, Inc.: Income Statement*, YAHOO! FIN., https://finance.yahoo.com/quote/FB/financials [https://perma.cc/MS8U-YNAP].

202. *See* CNBC Television, *supra* note 165.

203. *See* N.Y. GEN. BUS. LAW § 899-bb(2)(d) (LexisNexis 2021).

204. Joseph J. Lazzarotti, Jason C. Gavejian, Damon W. Silver, Mary T. Costigan & Delonie A. Plummer, *New York SHIELD Act FAQs*, 11 NAT'L L. REV. no. 143 (July 10, 2021), https://www.natlawreview.com/article/new-york-shield-act-faqs [https://perma.cc/29WV-MP7P].

205. *Id.*

requirements and its broad reach, the SHIELD Act does not provide a private right of action, but rather leaves this decision within the discretion of the New York Attorney General.[206] This mimics the federal scheme in that the FTC has the discretion to initiate prosecution under the FTC Act, so an individual consistently lacks a private right of action.[207] In the end, the user may be at the mercy of government officials for enforcing data management standards through legal action.

Even when there are federal and state statutes that govern the handling of user information and may provide a cause of action against commercial entities, these statutes are typically limited in scope.[208] For instance, the Gramm Leach Bliley Act ("GLBA") of 1999 forbids entities from "disclos[ing] nonpublic personal information" unless certain conditions are met.[209] However, the GLBA applies to financial institutions; thus social media companies are not within its scope.[210] To fill this void, legislation in some states covers information gathered by social media companies.[211] For example, as previously mentioned in Section II.C, BIPA in Illinois protects *biometric* information collected by companies, which implicitly limits information to health data considered "biometric."[212] The state statute that arguably provides the most protection is the CCPA, enacted in California.[213] At the time of enactment, it was "the most comprehensive privacy legislation in the United States, with extensive new compliance requirements and liabilities."[214] The CCPA "provide[s] privacy protections to individuals by granting them control and access to their . . . information" and a private right of action.[215]

While statutes may not provide individuals a cause of action to recover from poor data security or privacy practices, initiating legal action based on common law, in negligence and breaches of the platform's privacy policy, may fill some gaps. After a data breach or inadvertent disclosure of information occurs, companies must disclose that the incident took place and follow applicable state statutes to comply with methods and timing of notice and who

206. *Id.*

207. *See* Carlson v. Coca-Cola Co., 483 F.2d 279, 280 (9th Cir. 1973).

208. *See, e.g.*, 15 U.S.C. § 6801 (2018) (limiting enforcement of the Gramm-Leach-Bliley Act to financial institutions).

209. 15 U.S.C. § 6802(b)(1).

210. *See id.* §§ 6801, 6809(3).

211. *See* 740 ILCS 14/10 (West 2020) (including social media companies by broadly defining "biometric information" to be "any information, regardless of how it is captured"); *see also In re* Facebook Biometric Information Privacy Litigation, 185 F. Supp. 3d 1155, 1155 (N.D. Cal. 2016) (opining on class action lawsuit against Facebook, "alleging that operator unlawfully collected and stored biometric data derived from their faces").

212. *See* 740 ILCS 14/10.

213. *See* CAL. CIV. CODE § 1798.100–10 (West 2020); *see supra* note 105 and accompanying text.

214. Harwell, *supra* note 105.

215. *Id.*

to notify.[216] However, failure to comply with a data breach statute does not necessarily import a duty to safeguard that information in the first place.[217] As an alternative approach, plaintiffs may successfully bring a negligence or breach of implied contract claim against the company that was originally given that information.[218] Courts have allowed plaintiffs, for example, to maintain a negligence action by showing that when a company violates Section 5 of the FTC Act that violation is negligence *per se*.[219] Lastly, users may have recourse against social media companies for violating the platform's privacy policy through litigation. It is possible for a user to support a finding that a social media company violates his or her privacy through a violation of the platform's privacy policy, but the user must show that the company did not notify the user of a certain practice or that the company breached its own policy.[220] Additionally, users may be able to show the platform violated privacy due to a mass sharing of information.[221] Courts have declined to dismiss claims for breaching an implied contract where there was a relationship between the plaintiff user and the defendant platform and the defendant had a duty to protect the plaintiff's information.[222]

In an attempt to mitigate this issue, there are pending legislations racing to be the first comprehensive federal privacy act, but nothing has come close to enactment.[223] In 2019, there were multiple efforts to propose a federal law that would, among other things, create an administrative unit under the FTC to enforce privacy laws, set reasonable data security standards, and provide individuals with the ability to access or delete their personal information.[224] Unsurprisingly, passing a bill has been hindered by the debate over what the bill should contain, such as state law preemption and what industries to

216. *Security Breach Notification Laws*, NAT'L CONF. STATE LEGIS. (Apr. 15, 2021), https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [https://perma.cc/97HD-EMFH].

217. *See* Perdue v. Hy-Vee, Inc., 455 F. Supp. 3d 749, 759–60 (C.D. Ill. 2020) (outlining how the duty to notify of a breach did not indicate there was also a duty to safeguard information).

218. *See id.* at 760–61, 764; *see also In re* Equifax, Inc., Customer Data Sec. Breach Litig., 362 F. Supp. 3d 1295, 1327 (N.D. Ga. 2019).

219. *See Perdue*, 455 F. Supp. 3d at 760–61; *see In re Equifax*, 362 F. Supp. 3d at 1327.

220. *See* Austin–Spearman v. AARP, 119 F. Supp. 3d 1, 10–11 (D.D.C. 2015) (ruling that a company notified a user of the platform's privacy policy and what would happen to the data; thus, by negative inference, failure to notify could constitute breaching the privacy policy and violating a user's privacy).

221. *See generally In re* Facebook, Inc., Consumer Priv. User Profile Litig., 402 F. Supp. 3d 767 (N.D. Cal. 2019) (holding that users survived a motion to dismiss by sufficiently alleging they did not consent to "massive information sharing").

222. *See Perdue*, 455 F. Supp. 3d at 764.

223. *See* Social Media Privacy Protection and Consumer Rights Act of 2019, S. 189, 116th Cong. (2019) (pending for further discussion since January 17, 2019); American Data Dissemination Act of 2019, S. 142, 116th Cong. (2019) (pending for further discussion since January 16, 2019).

224. Zhang, *supra* note 76.

cover,[225] and Congress's attention constantly shifts its focus to more pressing issues, like addressing economic relief due to COVID-19.[226] Even though there is a general consensus among politicians and lawmakers that there is a national policy interest to have national data security law,[227] consumers cannot use this consensus as protection from the mishandling of their data.

Altogether, creating a social media profile implicates the bargaining power of social media companies over users who possess a desire to use social media. In attempts to promote harmony between the users and platforms, there have been minute changes in business practices and a lack of successful legislative initiatives. However, the totality of these circumstances fails to re-balance the dynamic between the platforms and users or give some control back to the user. To ignite progress towards a more equal relationship and address the lack of legislation, implementing a technical solution like self-sovereign identity ("SSI") will enable a user to have more control over the data shared and to what extent, while simultaneously providing a legal solution to govern that data-sharing relationship and provide the user with causes of action.

IV. SELF-SOVEREIGN IDENTITY AND HOW TO BE SOCIAL PRIVATELY

Users currently have two options when it comes to using social media: (1) continue using the platform and subject themselves to potential privacy risks; or (2) delete the profile(s) but use the services to the extent the platform allows without a registered profile to avoid privacy violations.[228] This Section outlines how, instead of the current "either or" situation, a technical solution can strike the balance between a platform's consumption of information and the users' desire to maintain privacy and control over that information. The theory of SSI combined with the structure of blockchain could enable a user to control what information is delivered to a platform and legally maintain that control. This solution prevents the platform from sharing information beyond what is permitted, thus balancing the relationship between a single user and an immense social media company. In effect, this solution provides tangential, but necessary, benefits: it increases a user's awareness over what information a platform is sharing; enhances the consensual use of data and establishes a more clear-cut case for reasonable expectations of privacy; improves traceability so users may track how companies handle user data and thus easily identify when information was

225. Martin Matishak, *After Equifax Breach, Anger but No Action in Congress*, POLITICO (Jan. 1, 2018, 7:39 AM), https://www.politico.com/story/2018/01/01/equifax-data-breach-congress-action-319631 [https://perma.cc/92YY-H5YV].

226. Jennifer Bryant, *2021 'Best Chance' for US Privacy Legislation*, INT'L ASS'N PRIV. PROS. (Dec. 7, 2020), https://iapp.org/news/a/2021-best-chance-for-federal-privacy-legislation [https://perma.cc/ZFX6-6TMP].

227. *See id.*

228. *See supra* notes 29–33 and accompanying text.

inappropriately shared; and is inherently secure, possibly eliminating the need for future technical security laws.

A. SELF-SOVEREIGN IDENTITY AND HOW TO USE IT IN SOCIAL MEDIA

The SSI theory promotes the values of control and autonomy, and when used in a commercial setting, it enables the user to provide only the necessary amount of information required to complete a transaction.[229] When applied to interactions with social media companies, the user can retain control over their identity. Companies, on the other hand, are not entirely shut out from accessing data the user approves. This brings some harmony to the relationship between the user and the platform.

As an alternative identity framework, SSI allows users to exercise more control over their information and shift data management back to the users compared to the current framework.[230] Typically, social media users must create a separate profile for each platform to fully consume its services.[231] In effect, this requires the user to duplicate efforts to enter personal information and potentially manage several identities.[232] While the information may originate from the user, the profile can be perceived as owned by the platform.[233] Additionally, that information is stored in the database of a given platform and could be shared further with business partners. As the number of locations of data are increased, the possibility of exposure is consequently

---

229. *See, e.g.*, Tracy Molino, *Practical Application of Distributed Ledger Technology: Self-Sovereign Identity on the Blockchain*, JD SUPRA (Oct. 23, 2019), https://www.jdsupra.com/legalnews/practical-application-of-distributed-71041 [https://perma.cc/R79N-ZBNV] ("[Individuals] can choose to provide select data points about themselves under conditions that they set when there is a need for such information collection, without having to rely on a central repository to store this information. For example, [a person] may want a prospective employer to have access to information about [his or her] educational qualifications and previous work history, but not see that [he or she is] the president of . . . [a] fan club." (footnotes omitted)).

230. Christopher Allen, *The Path to Self-Sovereign Identity*, LIFE WITH ALACRITY (Apr. 25, 2016), http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html [https://perma.cc/8AE3-RXCK].

231. Platforms occasionally allow users to import an existing profile. *See supra* notes 35–36. When this occurs, platforms initially share information to establish a profile and continue to do so while there is integration. *See id.*

232. *Online Identity in 2040—Scenario Building with Self-Sovereign Identity*, SSI AMBASSADOR (Jan. 18, 2020), https://ssi-ambassador.medium.com/online-identity-in-2040-scenario-building-with-ssi-ab680c03b967 [https://perma.cc/ZAB9-DHWB] [hereinafter *Online Identity*, SSI AMBASSADOR] ("The average user already owns 7[.]6 social media channels with countless more logins for other online services."); *see also* SSI Ambassador, *An Introduction to Self-Sovereign Identity*, YOUTUBE (June 12, 2019), https://www.youtube.com/watch?v=djhYZZ3CkuM [https://perma.cc/DT3M-79N5] [hereinafter *Introduction*, SSI Ambassador] (describing how a person with multiple profiles has created multiple personas).

233. *Google Terms of Service*, GOOGLE, https://policies.google.com/terms?hl=en&fg=1#toc-problems [https://perma.cc/AZ7Z-Q7XF] [hereinafter *Google Terms*] (explaining how Google can suspend an account from accessing the platform's services implying a user does not have full ownership).

increased. In the end, the user creates and maintains an identity made up of their information and other content they share, for example, relationship status, hobbies, occupation, or education.[234]

1. SSI–The Concept

SSI is an identity management approach that can reframe and redefine the existing identity management mechanisms.[235] SSI is a concept which puts the user at the center of their identifying information with sole control and administration, effectively giving the user autonomy.[236] The user has the authority to determine how and with whom the data is shared, potentially limiting the disclosure of data elements.[237] These data elements can include PII as well as attributes, such as gender, university degree, or citizenship.[238] To initiate this model, the user must have accurate and verifiable information.[239] This presents the "trust triangle"[240] or "trust model"[241] where there is a "flow of information between parties involving digital identification."[242] In this model, the user, known as the holder, manages the credentials and shares them with another party, known as the verifier, for a transaction.[243] The verifier can confirm the information by connecting with or trusting a third party, known as the issuer.[244] The holder, verifier and issuer make up the three corners of the "trust triangle." For instance, a police officer may request to see a person's driver's license. The police officer can process the license through a police database but knows the information has a high level of trust since it is a government-issued, verifiable credential.

---

234. Alexis Hancock, *Digital Identification Must be Designed for Privacy and Equity*, ELEC. FRONTIER FOUND. (Aug. 31, 2020), https://www.eff.org/deeplinks/2020/08/digital-identification-must-be-designed-privacy-and-equity-10 [https://perma.cc/C9J5-7GDG].

235. *See* Molino, *supra* note 229 (describing how Sierra Leone is collaborating with a not-for-profit to experiment with distributed ledger technology and provide Sierra Leone citizens with a digital identity to access "affordable credit and financial services").

236. Allen, *supra* note 230.

237. Adrian Doerk, *An Introduction to Self-Sovereign Identity. (SSI)*, SSI AMBASSADOR (Oct. 6, 2019), https://ssi-ambassador.medium.com/an-introduction-to-self-sovereign-identity-ssi-916eb42f0490 [https://perma.cc/SK4J-C9PJ] ("It gives individuals . . . agency to control their identity information . . . .").

238. *Id.*

239. *Id.* (explaining how a user with an identification card provided by a government entity has an identity and information elements which can be used by third parties to verify the person is who he or she claims to be).

240. *Id.*

241. Hancock, *supra* note 234.

242. *Id.*

243. Doerk, *supra* note 237.

244. *Id.*

2. The Blockchain Method

One method of implementing SSI is through blockchain, which can help the user realize enhanced control and security over information.[245] Blockchain, or a distributed ledger database, is cryptographic implementation by a network of distributed digital ledgers relying on computers, or nodes, for maintenance and does not require complete trust between each node.[246] Blockchain records each transaction, creating a block with a unique algorithmically generated value or key, and these blocks can trace to previous blocks, thereby creating the chain.[247] One important aspect of blockchain is decentralization; in other words, the blocks are not stored or owned in one location.[248] Depending on what type of blockchain is implemented, users may be able to see the full transaction history or the history may be limited to those users who are parties to the transaction.[249] Additionally, blockchain adds a level of security because a chain records every transaction, making it tamper-resistant since changes would be evident.[250] Lastly, the blockchain can be public or private.[251] Where data in a chain is publicly available, similar to the internet, it is a public blockchain, whereas a private chain requires permission and data that is accessible only by authenticated users.[252] Combining SSI with blockchain provides a new and attainable identity management system tool. In general, users have identifiers that convey a unique identity, such as a passport number or a Social Security number.[253] With SSI, users have a single

245. Sarah Manski, *Distributed Ledger Technologies, Value Accounting, and the Self Sovereign Identity*, FRONTIERS IN BLOCKCHAIN (June 23, 2020), https://www.frontiersin.org/articles/10.3389/fbloc.2020.00029/full [https://perma.cc/2RRV-JN97] ("Blockchain is an emergent technology created to enable the transfer of value with increased transparency, efficiency, and security . . . . The self-sovereign infrastructure allows users to set boundaries regarding who has access to their data and maintain their privacy.").

246. Devon S. Connor-Green, *Blockchain in Healthcare Data*, 21 INTELL. PROP. & TECH. L.J. 93, 97 (2017).

247. *Blockchain*, BUILT IN, https://builtin.com/blockchain [https://perma.cc/5JSS-Y7JQ].

248. *Id.*

249. *Intro to Decentralized Identity Technology: How Does Blockchain Cryptography Work?*, FINEXTRA (Aug. 20, 2020), https://www.finextra.com/blogposting/19221/intro-to-decentralized-identity-technology-how-does-blockchain-cryptography-work [https://perma.cc/S7G2-RHZ3].

250. Steve Snyder, *The Privacy Questions Raised by Blockchain*, LAW360 (Jan. 14, 2019, 3:13 PM), https://www.law360.com/articles/1115579/the-privacy-questions-raised-by-blockchain [https://perma.cc/U663-WC8S].

251. *See* ERIC PISCINI, DAVID DALTON & LORY KEHOE, DELOITTE, BLOCKCHAIN & CYBER SECURITY. LET'S DISCUSS 3 (2017), https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-blockchain-and-cyber-security-lets-discuss.pdf [https://perma.cc/555C-STKD].

252. *Id.*

253. *See* Doerk, *supra* note 237.

decentralized identifier assigned to them, "[a] globally unique persistent identifier."[254]

This value could be generated by the government and emulate a person's Social Security Number.[255] This would capture the idea of the "trust triangle," because the user would have an assigned value from a trusted entity (like the government). Parties conducting business with the user can trust a person is behind the online account with this verifiable identity.[256] But with blockchain, these globally unique identifiers can link to more particular identifiers, like a characteristic of the person, and the entire chain or distribution network forms a full identity.[257] The user owns the unique values to each block and can elect to share the value with another party by providing access to that particular element.[258]

Moreover, to complete a transaction, a user needs a private key and a public key.[259] "Public and private keys are . . . analogous to an email address and password, respectively."[260] The public key acts as an address that the public can see,[261] and, similar to an email, allows other users to find each other.[262] "When someone decides to [enter into a transaction] . . . they must [sign in with] their private key."[263] Sending this private key helps to ensure the validity and security of the transaction. All the blocks in the chain work together to verify (or deny) the validity of the transaction, and upon validation, enter the transaction into the chain.[264] To see how this works, consider a scenario. Someone purchasing alcohol only needs to provide an attribute to the vendor that she is of age instead of providing her driver's

254. Drummond Reed et al., *Decentralized Identifiers: Core Architecture, Data Model, and Representations*, WORLD WIDE WEB CONSORTIUM (June 27, 2021), https://w3c.github.io/did-core/ [https://perma.cc/Y5QM-PZHW] (defining "decentralized identifier").

255. *See* Daniel J. Marcus, Note, *The Data Breach Dilemma: Proactive Solutions for Protecting Consumers' Personal Information*, 68 DUKE L.J. 555, 589 (2018) ("[E]ach person would receive a unique code called a 'blockchain hash' that would be imprinted on every digital transaction as a personal identifier.").

256. *See* Doerk, *supra* note 237 (outlining the trust triangle where financial institutions can trust a person's identity provided by the government, like a driver's license).

257. *See id.* (providing use cases to access alcoholic vending machines or scooter rentals).

258. *Id.*

259. *How Does Blockchain Work? Everything There is to Know*, COINTELEGRAPH, https://cointelegraph.com/bitcoin-for-beginners/how-does-blockchain-work [https://perma.cc/X6UV-NWTW] [hereinafter COINTELEGRAPH].

260. *What Are Public Keys and Private Keys?*, LEDGER ACAD. (Oct. 23, 2019), https://www.ledger.com/academy/blockchain/what-are-public-keys-and-private-keys [https://perma.cc/4GLU-G9FS] [hereinafter LEDGER ACADEMY].

261. *See* COINTELEGRAPH, *supra* note 259.

262. *See* LEDGER ACADEMY, *supra* note 260.

263. *See* COINTELEGRAPH, *supra* note 259.

264. *See id.* (describing how a user needs a digital signature in order to execute a transaction; once, the validity of the transaction is confirmed, the information is added to the chain).

license.[265] Otherwise, by handing over a driver's license, the vendor can read birthdate, address, weight, and height, all of which is more than necessary for the transaction. But based on the chain, this age can be verified by tracing it to the birthdate record.[266] Then, users, vendors, and government entities would be able to add authenticated information and attributes to the chain thereby creating a full online-accessible identity.[267] Because the user maintains ultimate control, the user is able to see if any party shares the key with someone since that transaction would be added to the chain.[268]

Lastly, combining SSI with PII offers interoperability and portability, meaning the same data elements can be shared in various contexts. For example, a user can provide her age to purchase alcohol or to rent a car, regardless of whether the parties are on different operating systems.[269] Notably, the solution might not need to be a fully developed blockchain; the implementation could emulate blockchain and only include a subset of components.[270] Thus, the blockchain could be built to the extent necessary to conduct online transactions and limit what information can be added.

The use of blockchain has already been deployed by some nations and is being tested by states as a way to manage a person's identity.[271] For example, Estonia uses the distributed ledger system.[272] In Estonia, each person "has a nationally-issued Estonia ID card for keeping track of public, financial, medical and emergency services."[273] In Illinois, there is a pilot project to test the effectiveness of a "'self-sovereign' identity for Illinois citizens on a distributed ledger" and "store government-verified attributes, such as legal name, date of birth, sex, and blood type."[274]

---

265. *Introduction*, SSI AMBASSADOR, *supra* note 232.

266. *See id.*

267. *See Introduction*, SSI Ambassador, *supra* note 232 (discussing how users can have attributes associated with their profile); *see also* Michael Mainelli, *Blockchain Could Help Us Reclaim Control of Our Personal Data*, HARV. BUS. REV. (Oct. 5, 2017), https://hbr.org/2017/10/smart-ledgers-can-help-us-reclaim-control-of-our-personal-data [https://perma.cc/3VM8-UXRB] (discussing how multiple parties can "share authoritative information").

268. *See* Matthew Hooper, *Top Five Blockchain Benefits Transforming Your Industry*, IBM (Feb. 22, 2018), https://www.ibm.com/blogs/blockchain/2018/02/top-five-blockchain-benefits-transforming-your-industry [https://perma.cc/ZA7C-FS23] (applying blockchain with commercial goods improves traceability because the technical solution provides "an audit trail that shows where an asset came from and every stop it made on its journey").

269. *See* Doerk, *supra* note 237.

270. *See* Roger A. Grimes, *What Blockchain Can and Can't Do for Security*, CSO (July 11, 2019, 3:00 AM), https://www.csoonline.com/article/3408317/what-blockchain-can-and-cant-do-for-security.html [https://perma.cc/77EY-9YDJ] (offering a distributed ledger as a "lightweight" version of blockchain and explaining how companies could benefit from using attributes of blockchain without implementing a full version).

271. *See* Molino, *supra* note 229.

272. Marcus, *supra* note 255, at 590.

273. *Id.*

274. *Id.* at 591.

3. Blockchain Use for Social Media Platforms

Taking the solution further than how it is currently implemented, users can employ this model when signing up for a social media platform. Theoretically, the entire distributed ledger would make up the profile of the user with particular data elements dispersed throughout the ledger. When a user signs up and creates an online profile, the user could give the platform access to particular data elements *a la carte*.[275] This way, the user can pick which data elements the user wants to share, give the social media platform the keys, or hash values, to those particular data elements, and the platform would not be able to take more.[276] A user could "forward . . . [information] to people who need to see it, while keeping control of access, including whether another party can forward the information."[277] A user could also "revoke someone's access to the information in the future."[278] With that in mind, the user can give the platform access to information on the condition that it is not distributed to an unauthorized party at the risk of having access revoked.[279] The user may also be able to program these conditions into the ledger through "smart contracts."[280] These contracts can be coded into the blockchain and embed the explicit conditions dictating when the data may be shared instead of trusting the other party to respect the conditions.[281] Thus, users could leverage SSI and blockchain to create a profile while increasing control, security, and management of their information.

B. CONSUMER AWARENESS AND CONTROL

With the current business model of engaging with social media platforms, the user essentially gives blanket permission to access information. With the SSI-blockchain combination, this solution would fragment the amount of data the user shares, thereby raising awareness on how much information a platform consumes and shift control towards the user.

As previously discussed in Section II.A, when a user creates an online profile for any given social media platform, the user categorically consents to the terms and services and the privacy policy.[282] The user does not have an opportunity to negotiate; if the user refuses, the user can abandon creating a

275. *See* Mainelli, *supra* note 267.

276. *See id.* ("[A] distributed ledger . . . may be unreadable if its contents are encrypted."). An entity wishing to access information on the ledger will need the encryption key to access the information. *See id.*

277. *Id.*

278. *Id.*

279. *Id.*

280. *See* Josh Stark, *Making Sense of Blockchain Smart Contracts*, COINDESK (June 7, 2016, 3:48 PM), https://www.coindesk.com/making-sense-smart-contracts [https://perma.cc/SLM2-CLFD].

281. *See id.* (outlining how smart contracts can be an "[a]lternative to traditional legal agreements" and code into the ledger when certain transactions may occur).

282. *See Twitter Terms of Service*, *supra* note 131; *see also Facebook Terms of Service*, *supra* note 45.

profile and use the basic services.[283] Instead, this proposed model would reshape how that process is executed. The user could select which data elements to give to the platform, such as name and date of birth, and refuse access to any other elements.[284] If the platform required or wanted more data elements, the platform would be forced to notify the user specifically which data elements it would need. The user would then have a foot in the door to "negotiate" with the platform and develop an agreement suitable for both parties, similar to the way websites track cookies.

As a result, the user is aware of what information the platform consumes, and the user could question the need for some data elements. If the platform provides a list of the data elements it will consume up front instead of providing a link to the privacy policy, the user will have actual knowledge of what information is being shared. When the user identifies a data element with which they do not feel comfortable sharing, the platform would be incentivized to provide more information about the need for that data. This transparency may comfort users and provide their information, otherwise persistent resistance will force the platform to rethink the use and need of data. This fosters a give and take between the platform and user. The communication does not need to be verbal or person-to-person; platforms could follow, for example, the approach websites use with cookies.[285] When a person visits a website, a banner may appear prompting the user to consent to cookies.[286] The user has an opportunity to accept or deny the request, and, in some cases, the user can "manag[e] cookie preferences" by denying access to some cookies while accepting others.[287] To facilitate this process, websites include descriptions of each cookie to inform the users of a cookie's

283. *See Create a New Account*, *supra* note 44 (clicking on "Create New Account" prompts a screen where a user can enter basic information to create a profile with text at the bottom stating: "[b]y clicking Sign Up, you agree to our Terms, Data Policy, and Cookies Policy," demonstrating that the user cannot reject the terms).

284. L. A. Capisizu, *Digital Identity*, 2020 CONFERINTA INTERNATIONALA DE DREPT, STUDII EUROPENE SI RELAT 256, 260 (2020) (Rom.) ("[T]he person has both the means to generate and control unique identifiers and also the facilities for stor[ing] the identity data. The person is thus free to share only the data he wants to transmit . . . .").

285. Alina Bradford, *3 Times You Shouldn't "Accept Cookies" on a Site*, READER'S DIG. (Sept. 21, 2020), https://www.rd.com/article/times-you-should-never-accept-cookies-on-a-site [https://perma.cc/6Q7V-KBLM] ("Cookies are . . . small text files stored on your browser by the sites you visit. . . . Cookies can . . . remember your shopping preferences so that you get a personalized experience when you visit [a] website.").

286. *Id.*

287. *Cookies & Other Tracking Technologies Notice*, UNIV. CORP. FOR ATMOSPHERIC RSCH. (July 2019), https://www.ucar.edu/cookie-other-tracking-technologies-notice [https://perma.cc/U58W-YDE8].

purpose.[288] For platforms, this approach could encourage or force the platform to provide an explanation and encourage transparency.[289]

The user is also afforded improved control over information because the user can restrict who has access as well as what information is shared. When the user creates a profile, they can permit the platform with access to particular data elements. During this transaction, the user can communicate to the platform that access is limited specifically to that platform. Even if this conversation does not take place, the platform will be on notice that the user can revoke access at any given time.[290] In either situation, if the platform shares information with a third party and the user does not want that party to have the information, the user has the ability to see that transaction occur[291] and revoke access.[292] Along the same lines, the user has more control by not providing certain data elements. The user will need to read the privacy policy to understand what data elements are used and for what purpose but could elect to withhold an element. If the platform absolutely requires the data element, it would be motivated to be as transparent as possible. Today, for example, a platform's terms and services may provide that it will collect the battery level of the device accessing the platform, or the IP address.[293] Yet, today, some users may choose to use a virtual private network ("VPN") to connect to a platform.[294] The VPN allows a user to change the IP address and encrypt the internet connection to secure the online activity.[295] Provided that a user can change their IP address and still access the platform, it demonstrates the lack of necessity for the IP address data element. With SSI, a solution like VPNs might not be required as a workaround. Also, platforms are able to operate without this information. In this way, SSI would be a sufficient replacement for VPNs since there would not necessarily be a distinction between hiding information versus withholding it. With the SSI model, the user can claw back some power and retain control over data elements the platform does not necessarily need.

---

288. *See id.*

289. *See #BrandsGetReal: Social Media & the Evolution of Transparency*, SPROUT SOC., https://sproutsocial.com/insights/data/social-media-transparency [https://perma.cc/76EZ-DM9X] (reporting survey results indicating that users "believe transparency from businesses is more important than ever before").

290. *See* Mainelli, *supra* note 267.

291. *See* COINTELEGRAPH, *supra* note 259 (providing that "[a]ll transactions occurring on a Blockchain are recorded there, so the transactions of any person using the network are public and completely transparent, even though they may be anonymous").

292. *See* Mainelli, *supra* note 267.

293. *See Data Policy*, FACEBOOK, *supra* note 51 (outlining under "Device Information" the information Facebook collects from the devices accessing its platform).

294. *See* Nadav Shemer, *10 Things You Need to Know About Using a VPN to Change Your Location*, TOP10.COM (Jan. 27, 2021), https://www.top10.com/vpn/geo-spoofing-how-to-fake-your-location-using-a-vpn [https://perma.cc/RZ9T-7LJR].

295. *Id.*

The SSI-blockchain approach does have a few flaws. First, the time potentially spent in creating a social media profile could be onerous, and negotiations could be difficult. First, while this approach increases the level of transparency around the amount of data a platform will request, the platform could generate a laundry list of data elements. If users have to comb through this list of data elements each time they want to create a profile, this exhaustive approach may dissuade users from using it and opting for the traditional blanket permission. If, however, the process was always an opt-in approach to data sharing, platforms would be incentivized to narrow their list to only the data they really need, therefore forcing them to be more efficient. Second, this approach would force the platform to negotiate with each user creating a profile, which, considering platforms have millions of users, might not seem to be a feasible or attractive solution.[296] Currently, every user creating a profile provides a generic template of information.[297] With this approach, platforms would have to reconsider how they would solicit information, decide which data elements are necessary, and manage settings for every user. With a vast number of users, the prospect of negotiating with each one can seem cumbersome. However, websites currently allow users to toggle which cookies the users will allow the website to track.[298] By comparison, this approach would not differ greatly from managing cookies—a user can toggle which data elements she plans to share.

Another overarching issue is that social media is meant to be social, and there must be a balance between privacy and being social. Users join social media platforms for a number of reasons and enjoy sharing content with other users.[299] Yet, the concept of privacy is inherently at odds with the concept of being social.[300] Naturally, there are compromises. Ideally, with a model promoting informed consent and control, the user is well aware of the compromises. After all, users would still like to use social media; the reckless disregard for their privacy and lack of trust by platforms makes them weary.[301]

---

296. *See* Tankovska, *supra* note 13.

297. *See supra* notes 34–38 and accompanying text.

298. *See* Alex Webb, *Google's Cookie Fight Will Shape Future of Digital Advertising*, BLOOMBERG BUSINESSWEEK (July 16, 2020, 3:00 AM), https://www.bloomberg.com/news/articles/2020-07-16/google-s-cookie-overhaul-could-reshape-the-digital-ad-industry [https://perma.cc/EG2G-ZCRP] ("The European Union's General Data Protection Regulation . . . had already started to unpick the cookie economy by giving citizens more control over their data and letting them opt out of ad-tracking efforts.").

299. *See* Smith, *supra* note 19.

300. *Compare Privacy*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/privacy [https://perma.cc/9TRC-JSGX] ("the quality or state of being apart from company or observation") *with Social*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/social [https://perma.cc/Q95W-N5EQ] ("marked by or passed in pleasant companionship with friends or associates").

301. *See* Lee Rainie, *Americans' Complicated Feelings About Social Media in an Era of Privacy Concerns*, PEW RSCH. CTR. (Mar. 27, 2018), https://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns [https://perma.cc/

C. THE IMPACT ON LEGAL ANALYSIS: CONSENSUAL USE OF DATA AND REASONABLE EXPECTATION OF PRIVACY

SSI united with blockchain promotes consensual use of data and balances a reasonable expectation of privacy in a social world, thereby building a firmer boundary as to when information is voluntarily divulged. Even though social media users enjoy what the platforms offer, a sense of anxiety and unease can surround the use of their personal information.[302] The current patchwork of data protection mechanisms and enforcement processes presents users with an uphill battle when litigating over the privacy of their information, but this technical implementation offers an opportunity for courts to confine analysis and boost predictability.

As seen earlier, the tort of invasion of privacy is currently difficult to prove against the current social media platforms.[303] However, under this model, the user provides specific consent over what information is shared, so the model could streamline legal analysis. In situations where the user expressly consents to sharing information, a privacy claim would be quick and simple to assess. The users are aware of what information they are sharing, measure the risks and benefits to sharing that information, and can anticipate what will happen with that data.[304] Therefore, the three elements of invasion of privacy—"'[(1)] private facts[;] [(2)] [those facts] were made public[;] and [(3)] the [subject of the facts] would be "highly offensive to a reasonable person'" if made public[305]—would be easy to prove.

But, at the same time, the user would have an easier claim to ascertain when data is misappropriated. When the user initially shares her data with the platform, she can attach conditions that the data elements will not be shared or used in a particular manner.[306] Here, social media users can intend only for the platform to have that data. If a platform disclosed that information to a third party, the user could show a privacy violation.[307] In the second case, a platform may abuse a user's trust and violate expectations of privacy. Today,

---

WN4R-G4GM] (finding that social media users "are anxious about all the personal information that is collected and shared and the security" and only "9% of social media users were 'very confident' that social media companies would protect their data").

302. *See id.*

303. *See supra* Section II.C.2.

304. *See supra* Section IV.B.

305. Grimes v. County of Cook, 455 F. Supp. 3d 630, 640 (quoting Karraker v. Rent-A-Ctr., Inc., 411 F.3d 831, 838 (7th Cir. 2005)). Some courts add an additional element which is to consider if "the matter is 'not of legitimate concern to the public.'" Martin v. Mooney, 448 F. Supp. 3d 72, 79 (D.N.H. 2020) (quoting Lovejoy v. Linehan, 20 A.3d 274, 276 (N.H. 2011)).

306. *See* Mainelli, *supra* note 267 (discussing how access to information may be revoked).

307. *See* Cain v. Redbox Automated Retail, LLC, 136 F. Supp. 3d 824, 835–837 (E.D. Mich. 2015) (holding plaintiffs did provide permission for defendants to disclose and share information within organization and with organization's partner). If a user explicitly provides that the platform does not have consent to share her information at all, then any form of disclosure would violate that consent.

platforms may take more data from a user than what a user might expect; a user may upload a photo and the platform may assess and store templates of facial features.[308] Under this SSI model, the user grants the platform access only to the data element. If the platform attempts to extract more, the user can swiftly demonstrate that the platform obtained data beyond what was allowed, by pointing to the transactions on the chain or showing what the platform did with it.[309] The user would then have an easier time meeting the third prong in the invasion of privacy—the subject of the facts being information to which a user did not consent or provide. In the end, the legal analysis simply entails what information the user shared and how it was used, and violations can be identified more easily with these situations.

Concurrently, the SSI-blockchain model presents a tangential benefit that may help a court analyze and promote a reasonable expectation of privacy. Since the term "privacy" has been defined differently depending on the context,[310] courts identify the right to privacy based on the context. But under this model, the court no longer needs to do so. This model promotes "information control" because the user has the authority to determine what personal information is shared with others.[311] While the preceding discussion shows situations where the users will have an expectation of privacy,[312] users will not have an expectation of privacy over content they publish online, for example, blog posts. Then, the court only needs to distinguish between the information at issue to determine if the privacy right applies.[313] Additionally, the SSI model mitigates issues courts have in accounting for the platform's privacy policy.[314] Over time, a platform's policy changes, so it may be impossible to assess which version of the policy is relevant.[315] The expectation of privacy promoted by this model would control that issue because the

308. *See Facebook Wins Preliminary Approval to Settle Facial Recognition Lawsuit*, REUTERS (Aug. 19, 2020, 9:53 PM), https://www.reuters.com/article/us-facebook-privacy-lawsuit/facebook-wins-preliminary-approval-to-settle-facial-recognition-lawsuit-idUSKCN25G08M [https://perma.cc/P87Q-VY44] (reporting on how Facebook collected and stored facial features of users without their consent).

309. *See* Mainelli, *supra* note 267 (describing distributed ledgers, or blockchain, as a "super audit trail").

310. *See supra* Section II.C.1.

311. Schafer, *supra* note 78, at 8.

312. Users will have an expectation of privacy over information they share with and intend only for the platform and information they deliberately withheld from the platform. *See supra* notes 289–93 and accompanying text.

313. *See In re* Facebook, Inc., Consumer Priv. User Profile Litig., 402 F. Supp. 3d 767, 782–83 (N.D. Cal. 2019) ("[T]here can be 'degrees and nuances to societal recognition of our expectations of privacy . . . .'" (citations omitted) (quoting Sanders v. Am. Broad. Co., 978 P.2d 67, 72 (Cal. 1999))). Instead of these "'degrees and nuances,'" there would be a more straightforward category of privacy. *Id.*

314. *See id.* at 790.

315. *Id.*

platform's consumption of the information would depend on what the user has stipulated, not the privacy policy.

D. ANCILLARY BENEFITS: INCREASED SECURITY, TRANSACTION TRACKING, BREACHING THE NEW MODEL, AND CALCULATING PENALTIES

Due to the nature of blockchain, this model also brings the added benefit of increased security through its inherent design and ability to track transactions. Because of the increased security, blockchain presents an opportunity to narrow the types of breaches to which users are subjected and, as an added benefit, potentially trim the need for federal legislation requiring standard security. Finally, by separating a user's information throughout the distributed network, it would be easier to calculate penalties when a breach occurs.

As a distributed ledger, blockchain provides security enhancements over current models of data management. The traditional system of storing and managing information relied on a central database where all the information was located and accessed in one place.[316] In contrast, blockchain decentralizes this information and removes the central component.[317] Based on the inherent design or implementation, blockchain provides mechanisms to protect the confidentiality, integrity, and availability of the stored data.[318] Users can trace transactions "to a specific time period," which provides genuine assurance and makes the system reliable.[319] Additionally, the information can be fully encrypted, thereby ensuring security.[320]

However, some limitations exist. For instance, a key management system to govern how private keys are stored and accessed would need to be developed. Blockchain also requires implementing added layers of security. Software development standards would need to be implemented and overseen in order to address the functions blockchain introduces.[321]

Assuming the added layers of security are implemented, the model would cement which data issues are the most prevalent. How blockchain is implemented to manage a user's personal information consequently solidifies the primary concern of how the data is treated—the primary concern becomes how a platform itself handles the information. Because this model enables users to exert more control and limit how information is shared, a platform misappropriating information would be the type of data breach or

316. *See* Mainelli, *supra* note 267 (comparing the distributed ledger system to the central database).

317. *See id.*

318. *See* PISCINI et al., *supra* note 251, at 4 (discussing the benefits blockchain provides in the cyber security context).

319. *Id.* at 8.

320. *See id.* at 6.

321. *See id.* at 6, 8.

misuse attracting the most attention.[322] Data breaches stemming from hackers, for instance, while still paramount, would be a secondary concern.

Most existing and proposed legislation focuses on requiring systems to maintain reasonable security measures commensurate with the type of user information and protect it from unauthorized disclosure,[323] but using the distributed ledger could instigate legislation to tailor the scope of these laws. Most, if not all, existing state legislation requires social media platforms to take reasonable precautions based on the type information the entities store.[324] Proposed federal legislation follows a similar scheme.[325] While this approach does not discriminate against the type of technology used, it presupposes that the technology is insecure by itself and security must be added.[326] Yet, by comparison, blockchain has security features inherent in the design, which helps to identify the existing gaps in security.[327] Thus, state or federal legislation could be tailored in the social media context to require platforms to add specific security protocols to blockchain, potentially addressing the security concerns over a user's privacy.

With streamlined legal analysis,[328] there would be reduced effort to calculate penalties. In the distributed ledger, the user's information is dispersed throughout the nodes, or computers, composing the ledger. The user can assign various sensitivity levels of PII to the nodes. For instance, name and age could be on one node while date of birth, address, and sexual identity could be on another. Accordingly, these nodes can be assigned monetary values.[329] When a platform misappropriates or breaches this information, the

322. *See* Suranga Seneviratne, *The Ugly Truth: Tech Companies are Tracking and Misusing Our Data, and There's Little We Can Do*, CONVERSATION (Nov. 25, 2019, 11:33 PM), https://theconversation.com/the-ugly-truth-tech-companies-are-tracking-and-misusing-our-data-and-theres-little-we-can-do-127444 [https://perma.cc/H4DV-QQ2Q] (summarizing a report recording how users felt more uncomfortable with the way their data was handled compared to security measures a company takes, thus demonstrating that users are more with data misuse).

323. *Data Security Laws: Private Sector*, NAT'L CONF. OF STATE LEGISLATURES (May 29, 2019), https://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx [https://perma.cc/V9JT-UDFC].

324. *See id.*

325. *See* Consumer Online Privacy Rights Act, S. 2968, 116th Cong. § 107 (2019) (requiring covered entities to maintain "reasonable data security practices").

326. *See, e.g.*, Chris Hallenback, *What New Cybersecurity Legislation Doesn't Include*, SEC. BOULEVARD (June 30, 2020), https://securityboulevard.com/2020/06/what-new-cybersecurity-legislation-doesnt-include [https://perma.cc/DDU3-78H3] ("All of these cybersecurity legislative efforts have merit. The problem is that most of the proposed bills seeking to address ongoing challenges . . . do not cover the fundamental problems. . . .").

327. *See generally* PISCINI et al., *supra* note 251 (discussing the inherent security benefits blockchain provides while outlining precisely which security mechanisms need to be added).

328. *See supra* Section IV.C.

329. *See* Pauline Glikman & Nicolas Glady, *What's the Value of Your Data*, TECHCRUNCH (Oct. 13, 2015, 6:00 PM), https://techcrunch.com/2015/10/13/whats-the-value-of-your-data [https://perma.cc/8D2X-CGRA] (calculating personal information, such as age and sex, on the broader global market to cost $0.0007).

value to the user could be efficiently calculated by courts or agencies by referring to the node's value or, alternatively, using existing legislature to quantify a value.[330] In addition to the negative publicity platforms receive when this transaction occurs, they could anticipate the monetary penalty.

One issue with the model is the implementation, particularly implementing a scalable solution and talent.[331] First, the scale of blockchain may present a hurdle because of the amount of data to process.[332] As the blockchain grows larger, more data will be stored on the chain.[333] Whenever a user wants to add a transaction to the chain, the entire chain needs to be processed, and over time, this poses run-time issues.[334] Second, blockchain is relatively new technology. There is a lack of a talent pool and not many universities offer courses teaching students how to build a blockchain.[335] If an organization wants to implement this solution, the organization will have to spend time and money training employees or offer competitive salaries to the small pool of experts.[336] However, these concerns can be mitigated. With regard to scalability, researchers and companies are already theorizing and developing ways to improve blockchain's performance.[337] While "there is . . . no method that can . . . solve this problem perfectly" yet,[338] there are numerous ways to experiment and implement a blockchain system that is tailored for social media. Additionally, there is precedent for academia to broaden their courses in response to technology. For example, Python is a type of programming language which was introduced in 1991.[339] Since then,

330. The Illinois legislature established a monetary value for the biometric information, and a technical solution could solidify that value. *See* 740 ILL. COMP. STAT. ANN. 14/20 (West 2020); *see also* Bobby Allyn, *Judge: Facebook's $550 Million Settlement in Facial Recognition Case is Not Enough*, NAT'L PUB. RADIO (July 17, 2020, 11:36 PM), https://www.npr.org/2020/07/17/892433132/judge-facebooks-550-million-settlement-in-facial-recognition-case-is-not-enough [https://perma.cc/XQZ4-7YTC] (reporting on a judge rejecting a $550 million settlement offer from Facebook and declaring the offer as a "98.75 percent discount . . . off of the amount that the Illinois legislature said might be due"). In a lawsuit between Illinois residents and Facebook where Facebook was alleged to have illegally captured and maintained biometric data, Facebook ultimately reached a settlement of $650 million to the impacted individuals. REUTERS, *supra* note 308.

331. Mark van Rijmenam, *7 Blockchain Challenges to be Solved Before Large-Scale Deployment*, MEDIUM (Sept. 25, 2019), https://medium.com/dataseries/7-blockchain-challenges-to-be-solved-before-large-scale-deployment-3e45b47eee6 [https://perma.cc/ZRN2-ZMC7].

332. *Id.*

333. *Id.*

334. *Id.*

335. *Id.*

336. *Id.*

337. Qiheng Zhou, Huawei Huang, Zibin Zheng & Jing Bian, *Solutions to Scalability of Blockchain: A Survey*, 8 INST. ELEC. & ELECS. ENG'RS 16,440, 16,442 (2020) (surveying approximately thirty-seven "popular solutions of solving scalability").

338. *Id.* at 16,452.

339. Carlos Soto, *How to Learn Python: A U.S. News Guide*, U.S. NEWS (Nov. 23, 2020, 2:04 PM), https://www.usnews.com/education/learn-python-guide [https://perma.cc/3AGA-7RD2].

there has been an abundance of online courses[340] and prestigious institutions[341] offering students the chance to learn a programming language. Thus, courses, online or in a classroom, designed to plug the gap in blockchain coding knowledge can be reasonably anticipated.

V. CONCLUSION

Social media platforms have grown prevalent, but that growth has also resulted in a growth of consuming data. As users create profiles and use the platforms, they have become, unwittingly or not, the source of much of that data. SSI promotes the principle that a person should be at the center of their information and only provide that which is necessary to complete a transaction. Blockchain, or a distributed ledger system, enables that theory to become a reality. It allows a user to limit what information is shared, increase awareness before sharing it, and track where their information travels. Even though social media technology allows users to connect with friends and families, there is both a desire to engage in a more private manner and a distrust in the platforms to respect that privacy.[342] Combining this with the fact that current legal boundaries and remedies for privacy violations might not be satisfactory for users, this model shifts a user's online presence towards one with more autonomy. Altogether, in the meantime, the legal issues regarding privacy that users experience while interacting online could be solved through a technical solution like blockchain and SSI until the law matures.

340. *See id.*

341. *Introduction to Computer Science and Programming in Python*, MITOPENCOURSEWARE: MASS. INST. TECH., https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-0001-introduction-to-computer-science-and-programming-in-python-fall-2016 [https://perma.cc/MYT4-2U6D].

342. *See* Rainie, *supra* note 301 (reporting on individuals who would like to contain using social media but do not entirely trust platforms to protect their privacy).