2020

Realistically Reevaluating Social Media Data: The Privacy Paradox and the Possibility of Propertization

Thomas J. Gordon

INTRODUCTION

Imitation is no longer the sincerest form of flattery. Just ask Jessica. Jessica, 17, was enjoying her final carefree days as a high school senior in Minnesota when she discovered that there was someone purporting to be her on social media – same name, same picture, same biography.[1] That Jessica, however, was much darker. She was posting pornographic content, pushing Canadian real estate, and pitching Ghanaian cryptocurrency. The real Jessica immediately reported the account to Twitter, but it would take two years for the platform's security algorithm to finally flag and suspend the account.[2] The following year, the New York Attorney General took an unprecedented step and became the first state authority to hold the "troll factory"[3] responsible for digital deception accountable for stealing and selling personal data from 55,000 people, including minors.[4] Unfortunately, this cautionary tale came too late.

Two weeks after Jessica publicly shared her ordeal with *The New York Times*, the United States Department of Justice unsealed an indictment alleging Russian "specialists"[5] at a factory called Internet Research Agency ("IRA") had stolen the identities of 87 million Facebook users[6] with the help of a political data mining firm associated with the Trump campaign, Cambridge

---

[1] Nicholas Confessore et al., *The Follower Factory*, N.Y. TIMES (Jan. 27, 2018), www.nytimes.com/interactive/2018/01/27/technology/social-media-bots.html.

[2] *Id.*

[3] The term refers to large, centralized units that focus on producing disinformation and participating on social media. *See, e.g.*, Neil MacFarquhar, *Inside the Russian Troll Factory*, N.Y. TIMES (Feb. 18, 2018), www.nytimes.com/2018/02/18/world/europe/russia-troll-factory.html (explaining the mechanics of the Russian government's largest troll factory).

[4] Press Release, N.Y. Att'y Gen., Groundbreaking Settlement with Sellers of Fake Followers and "Likes" on Social Media (January 30, 2019), www.ag.ny.gov/press-release/2019/attorney-general-james-announces-groundbreaking-settlement-sellers-fake-followers.

[5] *See* United States v. Internet Research Agency, et al., No. 1: 18-cr-00032-DLF, 2018 WL 914777 (D.D.C. filed Feb. 16, 2018).

[6] David Patrikarakos, *In 'Targeted,' Data is the Precious Coin of the Realm of Digital Robber Barons*, WASH. POST (Oct. 11, 2019), www.washingtonpost.com/outlook/in-targeted-data-is-the-precious-coin-of-the-realm-of-digital-robber-barons/2019/10/11/f1cff630-eaa0-11e9-9306-47cb0324fd44_story.html.

Analytica.[7] The operation had comprised a database consisting of five thousand data points on every Facebook user in the United States over the age of eighteen.[8] The factory employed behavioral and clinical psychologists[9] who sorted and fed the data to bots who then targeted users with divisive conspiratorial messages.[10] Masquerading as Americans, "specialists" worked in twelve hour shifts and were required to make 80 comments and 20 shares on Twitter and Facebook[11] in multiple languages.[12] The mandatory quota was orchestrated to take advantage of the algorithms of the social network sites ("SNSs"),[13] to ensure each divisive post would be classified as a "trend"[14] and placed it on a prominent list capturing the attention of a large audience for a short period of time.[15] The goal was to impair, obstruct and defeat "the lawful governmental functions of the United States," including the 2016 U.S. presidential election.[16] And impair they did. In the last three months of the U.S. presidential election, "fake news" generated almost 120% more shares, reactions, and comments on Facebook than actual current event coverage.[17]

Social media has shifted from being a niche "social" activity to a democratized daily deluge

---

[7] Andy Greenberg, *Mueller Indictment: Russian Trolls Stole Real US Identities to Fool Facebook*, WIRED (Feb. 29, 2018), www.wired.com/story/russian-trolls-identity-theft-mueller-indictment/.
[8] Patrikarakos, *supra* note 6.
[9] *Id.*
[10] *Id.*
[11] *See* MacFarquhar, *supra* note 3.
[12] *See* Ashley Nicolas, *Taming the Trolls: The Need for an International Legal Framework to Regulate State Use of Disinformation on Social Media*, 107 GEO L.J. ONLINE 36, 44 (2018).
[13] See Danah Boyd & Nicole Ellison, *Social Network Sites: Definition, History, and Scholarship*, 13 J. COMPUT. MEDIATED COMMUN. 210, 211 (2007) (defining SNSs as "web-based services that allow individuals to: [1] construct a public or semi-public profile within a bounded system, [2] articulate a list of other users with whom they share a connection, and [3] view and traverse their list of connections and those made by others within the system" and explaining that "[t]he nature and nomenclature of these connections may vary from site to site").
[14] Jarred Prier, *Commanding the Trend: Social Media as Information Warfare*, 11 STRATEGIC STUD. Q. 52 (2017).
[15] Sitaram Asur et al., *Trends in Social Media: Persistence and Decay*, ARXIV (2011).
[16] *See* Internet Research Agency, *supra* note 5.
[17] Craig Silverman, *This Analysis Shows How Viral Fake Election News Stories Outperformed Real News on Facebook*, BUZZFEED NEWS (Nov. 15, 2016), www.buzzfeednews.com/article/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook.

of news and activity.[18] Far from America's initial conception of a "marketplace of ideas,"[19] SNSs today are stacked with "fake news," disinformation[20] and misinformation.[21] Now, a relatively small number of individuals can disseminate massive amounts of "fake news,"[22] manipulate real news[23] in real-time,[24] and even develop doctored audio and visual news,[25] all with a standard camera and laptop. Initially conceived as a communication medium for a select portion of the population,[26] SNSs currently count 3.5 billion users,[27] with 288 million new users joining in the past year alone.[28] As of January 1, 2019, 45% of the world's population are on SNSs, with North America reporting the largest overall usage rate of 88.1% of the total population.[29] Within these swelling numbers are also the growing population of fake accounts, "bots," originating from "troll

[18] Andrew McClurg, *Kiss and Tell: Protecting Intimate Relationship Privacy Through Implied Contracts of Confidentiality*, 74 U. CIN. L. REV. 887, 889-91 (2006) (describing the Internet as a means to "a worldwide gossip mall" and positing that "[p]rivate individuals did not possess or have access to instruments for widely disseminating information").

[19] *See* Abrams v. United States, 250 U.S. 616, 630 (Holmes, J., dissenting) (explaining that "when men have realized that time has upset many fighting faiths, they may come to believe . . . the ultimate good desired is better reached by free trade in ideas—that the best test of truth is the power of the thought to get itself accepted in the competition of the market").

[20] Michael Landon-Murray et al., *Disinformation in Contemporary U.S. Foreign Policy: Impacts and Ethics in an Era of Fake News, Social Media, and Artificial Intelligence*, 21 PUB. INTEGRITY 512, 513 (defining disinformation as "intentionally false information to serve an objective").

[21] Landon-Murray et al., *supra* note 20 (defining as "simply incorrect information").

[22] MATTHEW BAUM ET AL., COMBATING FAKE NEWS (2017).

[23] Alina Selyukh, *Hackers Send Fake Market-Moving AP Tweet on White House Explosions*, REUTERS (Apr. 31, 2013), www.reuters.com/article/net-us-usa-whitehouse-ap/hackers-send-fake-market-moving-ap-tweet-on-white-house-explosions-idUSBRE93M12Y20130423 (reporting the official @AP Twitter account was hacked and tweeted that two explosions at the White House injured President Obama, causing U.S. markets to plunge).

[24] @BuzzFeed, *You Won't Believe What Obama Says in this Video!*, TWITTER (Apr. 17, 2018), www.twitter.com/buzzfeed/status/986257991799222272?.

[25] Supasorn Suwajanakorn et al., *Synthesizing Obama: Learning Lip Sync from Audio*, 36 ACM TRANS. GRAPH. (2017) (highlighting how students used A.I. to create visually convincing videos of President Obama saying things he had said before in a completely different context by feeding a neural network seventeen hours of footage from former addresses as 'training data').

[26] Simon Kemp, *Digital 2019: Global Internet Use Accelerates*, WE ARE SOCIAL (Jan. 30, 2019), www.wearesocial.com/blog/2019/01/digital-2019-global-internet-use-accelerates.

[27] David Meltzer, *Combating the Millennial Attention Span to Keep Your Team Engaged*, ENTREPRENEUR (Oct. 4, 2017), www.entrepreneur.com/article/297833.

[28] *Id.*

[29] Kemp, *supra* note 26.

factories." About 15% of Twitters active accounts, totaling 48 million, have been reported as fake[30] and Facebook has reported roughly 60 million fake accounts.[31]

From "fakes news" to filter bubbles, the Internet seems to be broken and the growing consensus[32] is that SNSs are to blame.[33] As the digital disease spreads, the deception devolves,[34] exacerbating extremist points of view courtesy of massive personal data breaches[35] used by increasingly realistic bots creating the appearance of public support.[36] The finely-tuned algorithms amplify extreme and outrageous speech[37] by manipulating common cognitive biases[38] and addicting us to the chaos.[39] With the arrival of "deep fakes," which allow audio and visual

[30] Onur Varol et al., *Online Human-Bot Interactions: Detection, Estimation, and Characterization*, ARXIV (2017).

[31] *Extremist Content and Russian Disinformation Online: Working with Tech to Find Solutions, Hearing Before the Comm. on Judiciary, Subcomm. on Crime and Terrorism*, 115th Cong. 134 (2017) (statement of Colin Stretch, Vice President and General Counsel, Facebook.

[32] *2019 Trust Barometer*, EDELMAN (Jan. 30, 2019) (finding 73% of people worry about fake news being used as a weapon and only 43% trust social media as a reliable source of information).

[33] *See, e.g.*, FRANKLIN FOER, WORLD WITHOUT MIND: THE EXISTENTIAL THREAT OF BIG TECH (2017); JONATHAN TAPLIN, MOVE FAST AND BREAK THINGS: HOW FACEBOOK, GOOGLE, AND AMAZON CORNERED CULTURE AND UNDERMINED DEMOCRACY (2017); SIVA VAIDHYANATHAN, THE GOOGLIZATION OF EVERYTHING: (AND WHY WE SHOULD WORRY) (2011).

[34] In 2016, one IRA "specialist" made an average of 2,442 Facebook posts a month. In 2019, IRA Facebook posts have tripled, averaging 8,900 posts in October alone, yielding more than 9.7 million interactions by over 1.7 million accounts. There is also evidence the IRA and other factories are now leveraging local individuals as proxies to create and post content and even paying to rent their social media accounts to do the same. *See e.g.*, Shelby Grossman et al., Stanford University Internet Observatory, *Evidence of Russia-Linked Influence Operations in Africa* (Oct. 29, 2019); Davey Alba & Sheera Frenkel, *Russia Tests New Disinformation Tactics in Africa to Expand Influence*, N.Y. TIMES (Oct. 18, 2019), www.nytimes.com/2019/10/30/technology/russia-facebook-disinformation-africa.html.

[35] Confessore et al., *supra* note 1.

[36] Robinson Meyer, *The Grim Conclusions of the Largest-Ever Study of Fake News*, THE ATLANTIC (Mar. 8, 2018), www.theatlantic.com/technology/archive/2018/03/largest-study-ever-fake-news-mit-twitter/555104/.

[37] Molly J. Crockett, *Moral Outrage in the Digital Age*, 1 NAT. HUM. BEHAV. 769, 771 (2017) ("[O]utrage-inducing content appears to be more prevalent and potent online than offline").

[38] Soroush Vosoughi et al., *The Spread of True and False News Online*, 359 SCI. 1146, 1150 (2018) (Finding in a SNSs study that "Falsehood diffused significantly farther, faster, deeper, and more broadly than the truth in all categories of information, and the effects were more pronounced for false political news . . . human behavior contributes more to the differ- ential spread of falsity and truth than automated robots do.").

[39] Kasey Panetta, *Top Strategic Predictions for 2018 and Beyond*, GARTNER (Oct. 3, 2017), www.gartner.com/smarterwithgartner/gartner-top-strategic-predictions-for-2018-and-beyond ("[By 2022] the majority of individuals in mature economies will consume more false information than true information.").

manipulation of real people,[40] the Internet is about to become much more insane. As one scholar says, "[T]hink of it as a destructive variation of the Turing test: imitation designed to mislead and deceive rather than to emulate and iterate."[41]

The 'Internet Age' of today is arguably the most profound transformation of information since the invention of the printing press. Whereas oil fueled the factories of the Industrial Age, personal data[42] is driving a veritable artificial intelligence ("A.I.") arms race[43] and the United States, with its inadequate privacy protections,[44] is the Wild West. SNSs have amassed massive reserves of users' personal data, some of which they pawn off on a veritable black market to "behind the scenes actors"[45] and some of which third parties simply steal.[46] It has become clear

---

[40] Samantha Cole, *There is No Tech Solution to Deepfakes*, VICE (Aug. 26, 2018), www.vice.com/en_us/article/594qx5/there-is-no-tech-solution-to-deepfakes.

[41] Danielle Citron & Robert Chesney, *Deepfakes and the New Disinformation War*, FOREIGN AFF. (Sept. 30, 2019).

[42] Jack Balkin, *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation*, 51 U.C.D. L. REV 1149, 1154 (2017).

[43] American companies alone are estimated to have spent over $19 billion in 2018 acquiring and analyzing consumer data. *See* Louise Matsakis, *The Guide to Your Personal Data (and Who Is Using It)*, WIRED (Feb. 13, 2019), www.wired.com/story/wired-guide-personal-data-collection/. For example. Google has made more than a dozen AI and robotics acquisitions, spending $500 million alone on the purchase of DeepMind, a British AI development company that defines its mission as "solv[ing] intelligence" by combining "the best techniques from machine learning and systems neuroscience to build powerful general-purpose learning algorithms," *see, e.g.*, Dan Rowinski, *Google's Game Of Moneyball In The Age Of Artificial Intelligence*, READWRITE (Jan. 29, 2014), www.readwrite.com/2014/01/29/google-artificial-intelligence-robots-cognitive-computing-moneyball/; Ingrid Lunden, *Google's DeepMind Acqui-Hires Two AI Teams In The UK, Partners With Oxford*, TECHCRUNCH (Oct. 24, 2014), www.social.techcrunch.com/2014/10/23/googles-deepmind-acqui-hires-two-ai-teams-in-the-uk-partners-with-oxford/; Adam Clark Estes, *Meet Google's Robot Army. It's Growing.*, GIZMODO (Jan. 22, 2014), www.gizmodo.com/a-humans-guide-to-googles-many-robots-1509799897.

[44] *See infra* Parts III.B.1-3.

[45] Edith Ramirez, Chairwoman, FED. TRADE COMM'N, *Opening Remarks at PrivacyCon 2017* (Jan. 12, 2017), www.ftc.gov/system/files/documents/videos/privacycon-2017-part-1/ftc_privacycon_2017__transcript_segment_1.pdf (discussing the increasing number of "behind the scenes" companies gathering personal data); FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY (2014), www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf (discussing how data brokers obtain consumer information).

[46] *See, e.g.*, Lily Newman, *Twitter Puts Profit Ahead of User Privacy—Just Like Facebook Did Before*, WIRED (Oct. 2, 2019), www.wired.com/story/twitter-two-factor-advertising/ (reporting 32.8 million Twitter credentials may have been leaked); BBC NEWS (Apr. 4, 2019), www.bbc.com/news/technology-47812470 (reporting on authorities finding a "massive cache of data on unsecured Amazon servers used by a Mexican social media firm"); Paul Grewal, Deputy Vice President and General Counsel, *Suspending Cambridge Analytica and SCL Group from Facebook*, FACEBOOK

that personal data is really the price that must be paid for use of the 'free' platforms.[47] Through manipulation of primal behaviors,[48] SNSs promote personal freedom of expression while simultaneously constraining and commodifying their users,[49] thereby making personal privacy become a paradox.[50] In a democracy with easily accessible anonymity,[51] bad actors face no real-life consequences for their digital deceptions[52] and there is no A.I. algorithmic accountability.[53] Conversely, individuals' SNSs data is somehow seeping from the digital realm to the real world. Colleges are collecting data about prospective students,[54] stores are employing statisticians to sift through data to predict purchases,[55] health insurance companies are relying on data to determine

(Mar. 16, 2018), https://about.fb.com/news/2018/03/suspending-cambridge-analytica/ (reporting Cambridge Analytica exposed private user information by violating Facebook's privacy platform); In addition to violations of privacy protocols, Facebook and Twitter have recently reported hackers have intentionally infiltrated their 'private' networks. *See* Guy Rosen, Vice President of Product Management, *Security Update*, FACEBOOK (Sept. 28, 2018), www.newsroom.fb.com/news/2018/09/security-update/(reporting that hackers exploited a vulnerability in Facebook's code affecting nearly 50 million accounts); Kate Conger et al., *Former Twitter Employees Charged with Spying for Saudi Arabia*, N.Y. TIMES (Nov. 14, 2019), www.nytimes.com/2019/11/06/technology/twitter-saudi-arabia-spies.html (reporting on how Saudi Arabian spies rose through the ranks of Twitter accessing "personal information and account data of Twitter customers that included users' telephone numbers and I.P. addresses").

[47] Mary Madden & George Gao, *Privacy and Cybersecurity: Key Findings*, PEW RESEARCH CENTER (Jan. 16, 2015), www.pewresearch.org/fact-tank/2015/01/16/privacy/ (reporting 91% of Americans say they have lost control over how personal information is collected with only 2% viewing them as "very secure").

[48] *See infra* Part II.

[49] *See*, DANIEL SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET 6 (2007) ("[A]s people use the freedom-enhancing dimensions of the Internet, as they express themselves and engage in self-development, they may be constraining the freedom and self-development of others – and even of themselves.").

[50] Lee Rainie, *Americans' Complicated Feelings About Social Media in an Era of Privacy Concerns*, PEW RESEARCH CENTER (Mar. 27, 2018), www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns ("When it comes to algorithms that underpin the social media environment, users' comfort level with sharing personal information depends heavily on how and why their data are being used.").

[51] Kasey Panetta, *Top Strategic Predictions for 2018 and Beyond*, GARTNER (Oct. 3, 2017), www.gartner.com/smarterwithgartner/gartner-top-strategic-predictions-for-2018-and-beyond (predicting by 2022, the majority of individuals in mature economies will consume more false information than true information).

[52] Eric Jardine, *The Dark Web Dilemma: Tor, Anonymity and Online Policing*, Global Comm'n on Internet Governance Paper Series, No. 21 (September 30, 2015), https://ssrn.com/abstract=2667711.

[53] *See infra* Parts III.B.1-3.

[54] Douglas MacMillan & Nick Anderson, *Student Tracking, Secret Scores*, WASH. POSt (Oct. 2, 2019), www.washingtonpost.com/business/2019/10/14/colleges-quietly-rank-prospective-students-based-their-personal-data (finding forty-four universities collecting data by tracking Web activity and then assigning predictive scores of likelihood of enrolling).

[55] Charles Duhigg, *Psst, You in Aisle 5*, N. Y. TIMES, Feb. 19, 2012, at MM30 (discovering Target employed

the appropriate level of care,[56] and prisons are deferring to algorithmic assessments regarding prisoners' bail.[57] All of which, currently, is perfectly legal in the United States.[58]

This paper seeks to develop a viable framework in response to these digital developments that secures personal social media data by first recalibrating the concept of personal privacy and then reconceptualizing it as property. Part II explains the science reinforcing the symbiotic, cyclical relationship between individuals and SNS platforms, the core of which is the reward center. As naturally social animals, humans have certain primal needs and SNSs afford unlimited access to their fulfillment while simultaneously increasing their own profits. The net result of this relationship has affectively commodified users,[59] without SNSs providing any compensation.[60]Advances in A.I., from trained algorithms to the more advanced self-learning neural networks, have afforded SNSs unprecedent access to audiences in depth and breadth, allowing for innovative and insidious means of user manipulation.

Part III address the paradox of privacy in regard to devising, implementing, and enforcing it as a legal right, particularly in a nation with competing equities. From its inception, the

---

statisticians to sift through buying records of women who had signed up for baby registries and then assigning them a pregnancy prediction score).

[56] Colin Lecher, *What Happens When an Algorithm Cuts Your Health Care*, VERGE (Mar. 21, 2018), www.theverge.com/2018/3/21/17144260/healthcare-medicaid-algorithm-arkansas-cerebral-palsy (reporting health insurance companies using Internet data tracking tools, called "instruments," used in informing decisions about care).

[57] *See generally* Fred Cate & Jane Winn, *The Failure of Fair Information Practice Principles*, *in* CONSUMER PROT. IN AGE OF "INFO. ECON." 37 (2006) (reporting an increasing number of jurisdictions are transitioning away from a monetary system to one dependent on risk-assessment algorithms).

[58] *See, e.g.*, FED. R. CIV. P. 34 advisory committee's note to 1970 amendment. ("The inclusive description of 'documents' is revised to accord with changing technology. It makes clear that Rule 34 applies to electronic data compilations. . . ."). *See generally* Gordon Gottsegen & Josie Colt, *How to Delete Your Facebook, Twitter, Instagram, and Snapchat*, WIRED (Mar. 20, 2018), www.wired.com/story/how-to-delete-your-facebook-instagram-twitter-snapchat.

[59] *See generally* Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. (1980) (explaining modern day privacy infringements manifest in the commodification of individuals).

[60] *See generally* LAWRENCE LESSIG, CODE: AND OTHER LAWS OF CYBERSPACE, VERSION 2.0 (2006) (advocating the use of property rights to protect privacy on the Internet).

amorphous concept of 'privacy' has been a reactionary afterthought in the American legal system.[61] The inherent tension in developing effective privacy laws in the United States for a fast-moving digital frontier is a foundational tension. The delineation between promoting collective progress[62] versus protecting individual determinism[63] is a precarious proposition. However, as SNSs continue to cross personal boundaries, using and misusing neuroscience to recklessly manipulate and profit off of their users,[64] the need to recalibrate antiquated regulatory processes with shifting social norms is crucial.[65] Part III provides a snapshot of where three government —the Federal Trade Commission ("FTC"), Congress, and the Supreme Court. currently stand on the issue of personal data privacy protections, providing insight into the current shortcomings of preexisting protections today.

Taking into account the science of SNSs, the contextual complexity of privacy protections, and the current, respective structural institutional constraints, Part IV proposes reconceptualizing personal social media data as private property. Reclassifying this digital data as personal property accurately reflects the psychology discussed in Part II and overcomes the challenges of Part III as it allows for definitive institutional and ideological parameters to be developed and applied. From this framework, recasting SNSs as information fiduciaries more accurately encapsulates the role of similarly situated others. Further, under this re-conception, the structurally solid, but rigid, legal institutions would have to make minimal changes within the preconceived property frameworks

---

[61] *See infra* Parts III.B.1-3.

[62] U.S. CONST. art. I, § 9, cl. 2 ("To promote the progress of science and useful arts, by securing for limited times to authors and inventors the exclusive right to their respective writings and discoveries.").

[63] U.S. CONST. amend. I ("Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.")

[64] *See infra* Parts II.A.-B.

[65] Omer Tene & Jules Polonetsky, *A Theory of Creepy: Technology, Privacy, and Shifting Social Norms*, 16 YALE J.L. & TECH. (2014).

and arguably would be more effective in their ex post roles.

I. THE SYMBIOTIC SCIENCE OF SOCIAL MEDIA

A.I. advancements have enhanced SNSs' effectiveness in engaging users, but the driving force to their success is the neurological need to intimate and socialize.[66] SNSs' continued success and profitability depend on scalability, which is driven by A.I. algorithms fueled by personal user data.[67] The more photos, videos, text, and audio users upload to SNSs, the more A.I. algorithms learn to "see"[68] what interests the individual user and the "smarter" these algorithms become. In turn, as timelines and newsfeeds become increasingly personalized[69] and user engagement is exponentially enhanced,[70] the A.I. algorithms reach a tipping point at which they no longer have to wait for the individual to feed them data, they can infer predicative individual behaviors on their

[66] *See* Sandra Blakeslee, *Cells that Read Minds*, N.Y. TIMES, Jan. 10, 2006, F00001 ("The human brain has multiple mirror neuron systems that specialize in carrying out and understanding not just the actions of others but their intentions, the social meaning of their behavior and their emotions."); *See also,* Kelly Dickerson et al., *The Role of the Human Mirror Neuron System in Supporting Communication in a Digital World*, 8 FRONT. PSYCHOL. 698 (2017).

[67] *See* Bruce Schneier, *A Taxonomy of Social Networking Data*, 8 IEEE SEC. & PRIV'Y 88 (Jul. 26, 2010), www.schneier.com/blog/archives/2009/11/a_taxonomy_of_s.html (defining "data" as: personal information given to SNSs that is required for individuals to register, information personally posted by users on SNSs' platforms, and personal information that is hidden from plain sight, but is collected by SNSs regarding individuals' activity on their platform).

[68] Will Oremus, *Who Controls Your Facebook Feed*, SLATE (Jan. 2, 2016) (explaining the Facebook algorithm assigns a "relevancy" score to every post it could possibly show a particular user at a particular point in time).

[69] Oremus, *supra* note 65 ("Once every possible post in your feed has received its relevancy score, the sorting algorithm can put them in the order that you'll see them on the screen. The post you see at the top, then, has been chosen over thousands of others as the one most likely to make you laugh, cry, smile, click, like, share, or comment.").

[70] *Id.* ("[C]licks, likes, shares, and comments are what make posts go viral, turn individual users into communities, and drive traffic to the advertisers that Facebook relies on for revenue.").

own.[71] Thus, the capabilities of SNSs today are truly difficult to understate.[72] Section A discusses the science propelling people to use SNSs and explain why engagement continues to increase in spite of privacy violations and deception. Section B reviews how SNSs have created code that mirrors and manipulates the human needs discussed in Section A and, thereby, have increased engagement and revenues.

A. The Individual

The role individuals play in the digital ecosystem, as both producers and consumers of personal information, is crucial to the success of SNSs.[73] Afterall, humans are posting the content and creating the data, not the SNSs.[74] Thus, it is important to understand what compels individuals to post.

Humans are naturally social beings with a fundamental need to belong and an inherent desire for social status.[75] Over time, the human brain has evolved neural wiring that rewards

---

[71] A.I. analyzes diverse, rich user data and assigns it unpredictable values in order to infer user preferences, sensitive attributes (e.g., race, gender, sexual orientation), and opinions (e.g., political stances), or to predict behaviors (e.g., to serve advertisements). *See* Brent Mittelstadt et al., *The Ethics of Algorithms: Mapping the Debate*, 3 BIG DATA & SOC'Y 1–2 (2016). *See, e.g.*, *Google Search Changes Tackle Fake News and Hate Speech*, BBC NEWS (Apr. 25, 2017), www.bbc.com/news/technology-39707642 ("Facebook announced it had begun to assign each of its users a reputation score, predicting their trustworthiness on a scale from zero to one. The methodology behind its scoring is unclear. Google has added new metrics to its ranking systems that should help to stop false information from entering the top results for particular search terms. Twitter is also assessing a user's reputation for credibility by the behavior of others in a person's network as a risk factor in judging whether a person's tweets should be spread.").

[72] Samanth Subramanian, *Inside the Macedonian Fake-News Complex*, WIRED (Feb. 5, 2017), www.wired.com/2017/02/veles-macedonia-fake-news.

[73] Tene & Polonetsky, *supra* note 65.

[74] Jonathan Zittrain, *Privacy 2.0*, 2008 U. CHI. LEGAL F. 65, 100 ("We live in an age in which many of us privately maintain records or record fragments on one another. Through peer-produced social networking services like Facebook or MySpace, we share these records with thousands of others, or allow them to be indexed to create powerful mosaics of personal data.").

[75] *See generally*, Roy Baumeister & Mark Leary, *The Need to Belong - Desire for Interpersonal Attachments as a Fundamental Human-Motivation.*, 117 PSYCHOL. BULL. 497 (May 1995) 497, 499-508.

behaviors that seek out stimuli of social value[76] and encourage social interactions.[77] Collectively, social rewards activate three areas of the brain: the ventral tegmental ("VTA"), the prefrontal cortex, and the ventral striatum.[78] Collectively referred to as the mesolimbic pathway, [79] the VTA projects neurotransmitters of dopamine to the nucleus accumbens ("NAcc"), located in the ventral striatum, each time a response to a stimulus results in a reward. [80] Over time, through a process called long-term potentiation, repeated reward responses create stronger associations and increase the intensity of responses.[81] The context and cadence in which dopamine is released and received has important implications because the brain automatically associates the preceding behavior with this reward.[82] Eventually, the simple anticipation of a reward in connection with that behavior will release dopamine[83] and doing so intermittently can turn the dopamine-triggering behavior into a habit.[84]

The human brain is malleable and not as steadfastly hard-wired as scientists once thought.[85]

---

[76] Cameron Anderson et al., *Is the Desire for Status a Fundamental Human Motive? A Review of the Empirical Literature.*, 141 PSYCH. BULL. 574, 579 (2015).

[77] Rebecca Von Der Heide et al., *The Social Network-Network: Size is Predicted by Brain Structure and Function in the Amygdala and Paralimbic Regions*, 9 SOC. COGN. AFFECT. NEUROSCI. 1962, 1963 (2014).

[78] *See, e.g.*, Sylvia Morelli et al., *The Neural Bases of Feeling Understood and Not Understood*, 9 SOC. COGN. AFFECT. NEUROSCI. 1890 (2014); Vasily Klucharev et al., *Reinforcement Learning Signal Predicts Social Conformity*, 61 NEURON. 140 (2009); Mitja Back et al., *Facebook Profiles Reflect Actual Personality, Not Self-Idealization*, 21 PSYCHOL. SCI. 372, 372–74 (2010) (finding participants were expressing and communicating real personality rather than promoting idealized versions of themselves).

[79] Sören Krach et al., *The Rewarding Nature of Social Interactions*, 4 FRONT BEHAV. NEUROSCI. 1 (May 28, 2010).

[80] Diana I. Tamir & Jason P. Mitchell, *Disclosing Information About the Self is Intrinsically Rewarding*, 109 PROC. NATL. ACAD. SCI. U.S.A. 8038 (2012) (explaining participants underwent fMRI scanning and a significantly greater response was observed in the NAcc bilaterally when disclosing one's own opinions and attitudes than when judging those of another and both the NAcc bilaterally and the VTA responded more strongly when disclosing beliefs about one's own personality traits than when judging others).

[81] Joe L. Martinez & Brian E. Derrick, *Long-Term Potentiation and Learning*, 47 ANNU. REV. PSYCHOL. 173 (1996).

[82] Matthias Gruber et al., *States of Curiosity Modulate Hippocampus-Dependent Learning via the Dopaminergic Circuit*, 84 NEURON. 486 (2014).

[83] Wolfram Schultz, *Dopamine Reward Prediction Error Coding*, 18 DIALOGUES CLIN. NEUROSCI. 23 (2016).

[84] Kelly McSweeney, *This is Your Brain on Instagram: Effects of Social Media on the Brain*, NOW (Mar. 17, 2019), https://now.northropgrumman.com/this-is-your-brain-on-instagram-effects-of-social-media-on-the-brain/.

[85] Julie Hamaide et al., *Neuroplasticity and MRI: A Perfect Match*, 131 NEUROIMAGE 13 (2016); *See generally*

Accordingly, the increasing individual use of and time spent on SNSs, with their unprecedent unlimited supply of social stimuli and rewards, [86] has caused individual and public identities to converge.[87] Although individuals, in general, feel freer to self-audit their presentation and interactions[88] on SNSs, such control empowers[89] the individual's converged conception of themselves. Thus, a SNSs profile is more than just a virtual representation. [90]

Individuals intuit the type of content that will conform best to the attitudes of their social

Christian Montag & Sarah Diefenbach, *Towards Homo Digitalis: Important Research Issues for Psychology and the Neurosciences at the Dawn of the Internet of Things and the Digital Society*, 10 SUSTAINABILITY 415 (2018).

[86] *See, e.g.*, Christian Ruff & Ernst Fehr, *The Neurobiology of Rewards and Values in Social Decision Making*, 15 NATURE REV. 549 (2014); Sylvia Morelli et al., *The Neural Bases of Feeling Understood and Not Understood*, 9 SOC. COGN. AFFECT. NEUROSCI. 1890 (2014); Vasily Klucharev et al., *Reinforcement Learning Signal Predicts Social Conformity*, 61 NEURON. 140 (2009); Daniel K. Campbell-Meiklejohn et al., *How the Opinion of Others Affects Our Valuation of Objects*, 20 CURR. BIOL. 1165 (2010); Christopher Davey et al., *Being Liked Activates Primary Reward and Midline Self-Related Brain Regions*, 31 HUM. BRAIN MAPP. 660 (2010); Keise Izuma et al., *Processing of Social and Monetary Rewards in the Human Striatum*, 58 NEURON. 284 (2008); Christoph Korn et al., *Performance Feedback Processing Is Positively Biased as Predicted by Attribution Theory*, 11 PLOS ONE (2016).

[87] Karolina Sylwester & Matthew Purver, *Twitter Language Use Reflects Psychological Differences between Democrats and Republicans*, 10 PLOS ONE (2015) (discovering that the psychological disparities among people with differing political orientations through individual word use on Twitter was resonant with previous research; liberals tend to place more emphasis on uniqueness and use more swear words, anxiety- and feeling-related words while conservatives value group association and their tweets contain more achievement and religion-related words); Danah Boyd, *Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life*, MACARTHUR FOUNDATION SERIES ON DIGITAL LEARNING –YOUTH, IDENTITY, AND DIGITAL MEDIA VOLUME 15 119, 129 (2008) ("Because of the intricate connection between offline and online social worlds, the audience that teens envision online is connected to their social world offline, or to their hopes about the possible alternatives online."); Dar Meshi et al., *The Emerging Neuroscience of Social Media*, 19 TRENDS IN COGN. SCI. 771 (2015) ("While the neural systems supporting these social cognitive processes have been studied extensively in the offline world, the online social media is comparatively new. However, experts continue to conclude that the digital world often mimics the offline social world and interactions within this online social network parallel offline social interactions."). *See generally* CHRISTINE HINE, VIRTUAL ETHNOGRAPHY (2000); Malene Charlottte Larsen, *Perspectives on Online Social Networking*, 35 SOC. COMP. MAG. (2007).

[88] *See, e.g.*, Liad Bareket-Bojmel et al., *Strategic Self-Presentation on Facebook: Personal Motives and Audience Response to Online Behavior*, 55 COMPUT. IN HUM. BEHAV. 788 (2016); Aaron Ben-Ze'ev, *Privacy, Emotional Closeness, and Openness in Cyberspace*, 19 COMPUT. IN HUM. BEHAV. 451 (2003).

[89] Katelyn McKenna & John Bargh, *Plan 9 From Cyberspace: The Implications of the Internet for Personality and Social Psychology*, 4 PERS. SOC. PSYCHOL. REV. 57 (2000).

[90] *See* Russell Belk, *Possessions and the Extended Self*, 15 J. CONSUM. RES. 139, 139 (1988); Russell Belk, *Digital Consumption and the Extended Self*, 30 J. OF MKTG. MGMT. 1101 (2014).

circle,[91] which reinforces pre-conceived notions.[92] Features of SNSs, such as automatically personalized information feeds, encourage engagement, but also facilitate an individual's descent into a digital ideological echo chamber,[93] otherwise known as a "filter bubble." [94] By catering to common cognitive biases[95] and creatively manipulating the code of SNSs news feeds, bots and other bad actors are impressively successful at normalizing their inflammatory ideas.[96] In a world that increasingly relies on SNSs as a primary source of information,[97] the absence of traditional media gatekeepers[98] allows for unfettered digital deceptions.[99]

B. The Platform

SNSs are ultimately businesses that succeed only through expanding audiences and their

[91] Hossein Derakhshan, *The Web We Have to Save*, MEDIUM (Jul. 14, 2015), https://medium.com/matter/the-web-we-have-to-save-2eb1fe15a426 (referring to this as the "tyranny of the novel and the popular").

[92] M. Mitchell Waldrop, *News Feature: The Genuine Problem of Fake News*, 114 PROC. NATL. ACAD. SCI. U.S.A. 12631 (2017) ("People prefer to consume news or entertainment that reinforces what they already believe. And that, in turn, is rooted in well-understood psychological phenomena such as confirmation bias—our tendency to see only the evidence that confirms our existing opinions and to ignore or forget anything that doesn't fit.").

[93] Waldrop, *supra* note 120 ("[A] Facebook or Twitter newsfeed is just confirmation bias backed with computer power: What you see when you look at the top of the feed is determined algorithmically by what you and your friends like . . . discordant information gets pushed further and further down the queue, creating an insidious echo chamber.").

[94] ELI PARISER, THE FILTER BUBBLE: HOW THE NEW PERSONALIZED WEB IS CHANGING WHAT WE READ AND HOW WE THINK (2011).

[95] *See* Baum et al., supra note 22; *see also* Soroush Vosoughi et al., *The Spread of True and False News Online*, 359 SCI. 1146, 1149 (2018) (finding "[f]alsehood diffused significantly farther, faster, deeper, and more broadly than the truth in all categories of information, and the effects were more pronounced for false political news than for false news about terrorism, natural disasters, science, urban legends, or financial information").

[96] *See, e.g.*, Brendan Nyhan & Jason Reifler, *When Corrections Fail: The Persistence of Political Misperceptions*, 32 POL. BEHAV. 303 (2010); Donal Flynn et al., *The Nature and Origins of Misperceptions: Understanding False and Unsupported Beliefs About Politics*, ADVANCES IN POL. PSYCH. (2017); Jacob Ratkiewicz et al., Ass'n for the Advancement of Artificial Intelligence, *Detecting and Tracking Political Abuse in Social Media*, FIFTH INT'L AAAI CONF. ON WEBLOGS AND SOC. MEDIA (2011) ("Bots are designed to amplify the reach of fake news and exploit the vulnerabilities that stem from our cognitive and social biases. For example, they create the appearance of popular grassroots campaigns to manipulate attention and target influential users to induce them to reshare misinformation.").

[97] Mark Cohen, *Law In The Age Of Social Media*, FORBES (Nov. 27, 2016), www.forbes.com/sites/markcohen1/2016/11/27/law-in-the-age-of-social-media/#42023fd31db8; *see also* Hunt Allcott & Matthew Gentzkow, *Social Media and Fake News in the 2016 Election*, 31 J. ECON. PERSP. 211 (2017) (reporting referral data shows "fake news" stories relied heavily on social media for traffic during the election).

[98] Citron & Chesney, *supra* note 41.

[99] DAVID PATRIKARAKOS, WAR IN 140 CHARACTERS: HOW SOCIAL MEDIA IS RESHAPING CONFLICT IN THE TWENTY-FIRST CENTURY (2017).

attention;[100] they are not in the social media business, they are in the data trade industry.[101] Thus, their success in selling these enviable enormous concentrated hives of attention to advertisers[102] is determined by their ability to satisfy individuals' primal social needs[103] through social cognition, self-referential cognition, and social reward processing.[104] A.I. algorithms, simply understood as self-learning codes fueled by user data, ensure and enforce these feedback loops.

Effectively grabbing the attention of users for advertisers, SNSs are required to increasingly demanding detailed data and enhance engagement.[105] Thus, it is unsurprising that the more active an individual is on a SNS, the more they feel connected,[106] fulfilled,[107] and gratified,[108]

---

[100] Tufekci, *supra* note 121 ("Facebook makes money, in other words, by profiling us and then selling our attention to advertisers, political actors and others. These are Facebook's true customers, whom it works hard to please.")

[101] DIG., CULTURE, MEDIA AND SPORT COMM., FINAL REPORT, 2017-19, HC 1630 (describing how Facebook traded access to user data in exchange for advertising buys); Gabriel Dance et al., *Facebook Offered Users Privacy Wall, Then Let Tech Giants Around It*, N. Y. TIMES, 1 (Dec. 19, 2018) (describing how personal data was traded among 150 companies without user consent).

[102] Jack Balkin, *Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society*, N.Y.U. L. REV. 1 (2004). ("The digital revolution made a different kind of scarcity salient. It is not the scarcity of bandwidth but the scarcity of audiences, and, in particular, scarcity of audience attention.")

[103] Natalya Bazarova & Yoon Hyung Choi, *Self-Disclosure in Social Media: Extending the Functional Approach to Disclosure Motivations and Characteristics on Social Network Sites*, 64 J. COMMUN. 635 (2014).

[104] Diana Tamir & Adrian Ward, *Old Desires, New Media*, *in* PSYCH. OF DESIRE 432; *see also* Matthew Pittman & Brandon Reich, *Social Media and Loneliness: Why an Instagram Picture May Be Worth More than a Thousand Twitter Words*, 62 COMP. IN HUM. BEHAV. 155 (2016) ("[T]he three primary psychological factors driving the continued use of Twitter, Facebook and Snapchat are: [1] comparison with other people, [2] feelings of trust and bonding, and [3] finding groups with attitudes and interests aligned with one's own.").

[105] Tufekci, *supra* note 121.

[106] Nicole Ellison et al., *The Benefits of Facebook "Friends:" Social Capital and College Students' Use of Online Social Network Sites*, 12 J. COMP.-MEDIATED COMM. 1143 (2007); Charles Steinfield et al., *Social Capital, Self-Esteem, and Use of Online Social Network Sites: A Longitudinal Analysis*, 29 J. APP. DEV. PSYCH. 434 (2008); Sebastián Valenzuela et al., *Is There Social Capital in a Social Network Site?: Facebook Use and College Students' Life Satisfaction, Trust, and Participation1*, 14 J. COMP.-MEDIATED COMM. 875 (2009); Gina Masullo Chen, *Tweet this: A Uses and Gratifications Perspective on How Active Twitter Use Gratifies a Need to Connect with Others*, 27 COMP. IN HUM. BEHAV, 755 (2011).

[107] Aqdas Malik & Marko Nieminen, *Uses and Gratifications of Digital Photo Sharing on Facebook*, 33 TELEMATICS AND INFORMATICS (2015) (finding that when SNSs users sbared personal photos on SNSs, they felt 'fulfilled' from the attention and affection).

[108] Chei Sian Lee & Long Ma, *News Sharing in Social Media: The Effect of Gratifications and Prior Experience*, 28 COMP. IN HUM. BEHAV. 331 (2012).

and the more likely they are to repeatedly engage with the platform.[109] For example, upon registering for a Facebook account, the notification center includes activities from an initial set of connections, which establishes the link to social reward.[110] The more a user uses the SNS, the more active the notification center becomes, establishing the expectation that anytime the user opens the application, they can reasonably expect to be rewarded.[111] Another example is the notification algorithm from the Facebook-owned company, Instagram. The algorithm is programmed to withhold "likes" on photos and to deliver them in larger clusters at once. This intentional cadence is meant to take advantage of psychological anticipatory rewarding while simultaneously encouraging habitual use through balancing negative and positive feedback signals.[112]

In the early days of SNSs, platforms were populated by content only from users' immediate friends and family as the algorithms were based on engagements statistics alone[113] and required structured data, meaning human manpower was required to interpret the data.[114] The more data that is collected, the smarter, faster and more accurate the algorithms become.[115] SNSs were quick

---

[109] Mike Allen, *Sean Parker Unloads on Facebook*, AXIOS (Nov. 9, 2017), www.axios.com/sean-parker-unloads-on-facebook-god-only-knows-what-its-doing-to-our-childrens-brains-1513306792-f855e7b4-4e99-4d60-8d51-2775559c2671.html (According to the founder of Facebook last year: "The thought process that went into building these applications, Facebook being the first of them, was all about: 'How do we consume as much of your time and conscious attention as possible?' … And that means that we need to sort of give you a little dopamine hit every once in a while, because someone liked or commented on a photo or a post or whatever. And that's going to get you to contribute more content, and that's going to get you… more likes and comments…. It's a social-validation feedback loop… exactly the kind of thing that a hacker like myself would come up with, because you're exploiting a vulnerability in human psychology.")

[110] Tracii Ryan et al., *The Uses and Abuses of Facebook*, 3 J. BEHAV. ADDICT. 133 (2014).

[111] *Id.*

[112] *60 Minutes: What is "Brain Hacking"?*, CBS NEWS (Apr. 9, 2017), www.cbs.com/shows/60_minutes/video/tH3KnkheO5s1zWLe3kApXT_iDti_xiVC/brain-hacking/.

[113] WAEL GHONIM & JAKE RASHBASS, TRANSPARENCY: WHAT'S GONE WRONG WITH SOCIAL MEDIA AND WHAT CAN WE DO ABOUT IT?, SHORENSTEIN CTR. ON MEDIA, POLITICS, & PUB. POL'Y (Mar. 3, 2018), www.shorensteincenter.org/transparency-social-media-wael-ghonim/.

[114] IAN GOODFELLOW ET AL., DEEP LEARNING (2016).

[115] Karl Manheim & Lyric Kaplan, *Artificial Intelligence: Risks to Privacy and Democracy*, 21 YALE J.L. & TECH. 106 (2019).

to discover that knowledge of people's personalities could be used to manipulate and influence them,[116] and began to alter their algorithms, which are today notoriously elusive, to achieve those results.[117]

Today, the engines of SNSs are advanced A.I. algorithms called "neural networks," which replicate the structure of neurons in the human brain.[118] Neural networks are arranged such that humans do not perceive their actual operation and do not get to fix the manner in which elements are weighed.[119] These unperceivable networks are capable of "deep learning," meaning they train themselves[120] by using probability theory to navigate uncertain and ambiguous data[121] and, thereby, increase their accuracy.[122] Similar to earlier algorithms, with more experience they gain, the 'smarter' they become.[123] Today, these advanced algorithms are so sophisticated they outperform human judgment.[124]

A.I. has exponentially widened the spigot by which SNSs continue to amass massive

---

[116] Jacob Hirsh et al., *Personalized Persuasion: Tailoring Persuasive Appeals to Recipients' Personality Traits*, 23 PSYCHOL. SCI. 578 (2012).

[117] Nausicaa Renner, *Memes Trump Articles on Breitbart's Facebook Page*, COLUM. J. REV. (Jan. 30, 2017), www.cjr.org/tow_center/memes-trump-articles-on-breitbarts-facebook-page.php.

[118] Jay Stanley, *The Dawn of Robot Surveillance*, AM. CIV. L. UNION (Jun. 17, 2019), www.aclu.org/report/dawn-robot-surveillance (noting researchers believe that by mimicking the underlying structure of the brain they will be better able to mimic the intelligent tasks performed).

[119] Quoc V. Le et al., *Building High-Level Features Using Large Scale Unsupervised Learning*, ARXIV (Jul. 12, 2012).

[120] *From Not Working to Neural Networking-Technology*, ECONOMIST (Jun. 23, 2016).

[121] GOODFELLOW ET AL., *supra* note 114.

[122] Larry Hardesty, *Explained: Neural Networks*, MIT NEWS (Apr. 14, 2017), www.news.mit.edu/2017/explained-neural-networks-deep-learning-0414.

[123] Natalie Wolchover, *New Theory Cracks Open the Black Box of Deep Neural Networks*, WIRED (Oct. 8, 2017), www.wired.com/story/new-theory-deep-learning/.

[124] Youyou et al., *supra* note 78 (finding computer-based models significantly more accurate than humans in a core social-cognitive task: personality judgment).

reserves of rich personal data,[125] doing so at the cost of users' personal privacy.[126] Further, as the symbiotic relationship between the data-dependent SNSs A.I. algorithms and the implicitly compliant users deepens with increased engagement,[127] new forms of digital deception, such as "deep fakes," are developed and deployed.[128]

II. THE PARADOX OF PRIVACY

With data as the new oil[129] and SNSs priming the pump courtesy of neuroscience,[130] the resulting commodification of users[131]calls into question individual's right to privacy. The largely unregulated SNSs have been permitted to violate and dictate new social norms as the audience of their oversight expands.[132] For example, more than one-fourth of the world's data is currently

---

[125] In 2016, YouTube announced the largest existence of a single dataset to date, consisting of content amassed from six million individual users content, organized and arranged into 4,800 categories. *See, e.g.*, Sudheendra Vijayanarasimhan & Paul Natsev, *Announcing YouTube-8M: A Large and Diverse Labeled Video Dataset for Video Understanding Research*, GOOGLE AI BLOG (Sept. 28, 2016), http://ai.googleblog.com/2016/09/announcing-youtube-8m-large-and-diverse.html; Sami Abu-El-Haija et al., *YouTube-8M: A Large-Scale Video Classification Benchmark* (Note: the initial announcement was subsequently reduced to 6 million).

[126] *See generally*, Jules Polonetsky & Omer Tene, *Privacy and Big Data: Making Ends Meet*, 66 STAN. L. REV. ONLINE (2013); Jacob Kastrenakes, *Google's Chief Internet Evangelist Says, "Privacy May Actually Be an Anomaly,"* THE VERGE (Nov. 10, 2013), www.theverge.com/2013/11/20/5125922/vint-cerf-google-internet-evangelist-says-privacy-may-be-anomaly.

[127] JONATHAN ZITTRAIN, *Privacy 2.0*, *in* THE FUTURE OF THE INTERNET-AND HOW TO STOP IT, 220 (2008) ("The more our identity is associated with our daily actions, the greater opportunities others will have to offer judgments about those actions.").

[128] "Deep fakes" come from a specific type of "deep learning" in which pairs of algorithms are pitted against each other in "generative adversarial networks," or GANS. *See generally*, Danielle Citron & Robert Chesney, *Deepfakes and the New Disinformation War*, FOREIGN AFF., Sept. 30, 2019.

[129] *Data is the New Oil*, ANA (Nov. 3, 2006), www.ana.blogs.com/maestros/2006/11/data_is_the_new.html (credited with the phrase "data is the new oil"); *Fuel of the Future*, 423 THE ECONOMIST, 14 (May 6, 2017) ("data has replaced oil as the world's most valuable resource"); Charlie Warzel, *Trump Is Tracking Your Phone*, N. Y. TIMES (Oct. 22, 2019), www.nytimes.com/2019/10/22/opinion/trump-privacy-2020.html ("We live in a world that's driven by data. It's often called "the new oil."); Vanian, *supra* note 57 ("Big Data is the new oil.").

[130] *See infra* Part I.

[131] *See, e.g.* Richard Jenkings, *How Much is Your Email Address Worth?*, THE DRUM (Apr. 9, 2012), www.thedrum.com/opinion/2012/04/04/how-much-your-email-address-worth (reporting a market rate of $89 per e-mail address); Lauren Feiner, *Reddit Users Are the Least Valuable of Any Social Network*, CNBC (Feb. 11, 2019), www.cnbc.com/2019/02/11/reddit-users-are-the-least-valuable-of-any-social-network.html (valuing Reddit users at $0.30); Jay R. Corrigan et al., *How Much is Social Media Worth? Estimating the Value of Facebook by Paying Users to Stop Using It*, 13 PLOS ONE (2018) (calculating a $1,000 per North American Facebook user).

[132] Julia Angwin et al., *Facebook Enabled Advertisers to Reach 'Jew Haters,'* ProPublica (Sept. 14, 2017),

governed by Facebook's Terms of Service.[133] SNSs' access to and oversight of such an unprecedented breadth and depth of individuals[134] has permitted the reshaping of traditional norms to better align with platform's profits.[135] This acquiescence ultimately stems from the United States' detrimental decision during the Internet's inception to prioritize accessibility of the internet over personal privacy concerns.[136]

Part II provides a contextual overview of the legal right to personal privacy in the United States by looking at both its' historical development and modern materialization. In understanding the foundation upon which the concept of privacy devoleped and the landscape in which its' protections currently exist, the necessisty to revaluate and redefine personal privacy becomes clear. In order to maintain economic superiority on the world stage, the United States must modernize personal digital safeguards akin to the rest of the Western world.[137] Section A traces the historical inceotion and development of the concept of personal privacy relative to technological developments. Section B takes a look at three of the most relevant regulatory institutions in regard

---

www.propublica.org/article/facebook-enabled-advertisers-to-reach-jew-haters (reporting Facebook allowed placement of ads targeting and excluding African Americans, mothers, disabled people, Jews, and other minorities).

[133] Catherine Buni & Soraya Chemaly, *The Secret Rules of the Internet*, VERGE (Apr. 13, 2016), www.theverge.com/2016/4/13/11387934/internet-moderator-history-youtube-facebook-reddit-censorship-free-speech.

[134] *See, e.g.* Milton Mueller, *Hyper-Transparency and Social Control: Social Media as Magnets for Regulation*, 39 TELECOMM. POL'Y 804 (2015); Jack Balkin, *The Three Laws of Robotics in the Age of Big Data*, 78 OHIO ST. L.J. (2017) 1217, 1223 ("[T]he problem is not the robots; it is the humans.").

[135] Clive Thompson, *I'm So Totally, Digitally Close to You*, N. Y. TIMES, at MM42 (Sept. 5, 2008) (quoting Mark Zuckerberg: "Facebook has always tried to push the envelope. And at times that means stretching people and getting them to be comfortable with things they aren't yet comfortable with. A lot of this is just social norms catching up with what technology is capable of. In essence, Facebook users didn't think they wanted constant, up-to-the-minute updates on what other people are doing. Yet when they experienced this sort of omnipresent knowledge, they found it intriguing and addictive. Why? Social scientists have a name for this sort of incessant online contact.").

[136] *See infra* Part II.B.1.

[137] *See, e.g.*, Mark Scott & Natasha Singer, *How Europe Protects Your Online Data Differently Than the U.S.*, N. Y. TIMES (Jan. 31, 2016), www.nytimes.com/interactive/2016/01/29/technology/data-privacy-policy-us-europe.html; Press Release, Eur. Comm'n, Facebook, Google and Twitter Accept to Change Their Terms of Services to Make Them Customer-Friendly and Compliant with EU Rules (Feb. 5, 2018), https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=614254.

to personal data privacy and assesses their relative current responses.

A. The Concept

Anonymity is foundational to the fabric of America,[138] the protection of which has immense individual and societal value by way of self-determination and democratic deliberation.[139] In an age when individual identity is automatically aligned with digital data, evaporating any autonomy one may have,[140] personal privacy has no definitive legal protection[141] or privilege.[142]

Personal privacy, like freedom, has always been difficult to define, yet definitive once

---

[138] *See* McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 368 & n.3 (1995) (Thomas, J., concurring) ("There is little doubt that the Framers engaged in anonymous political writing. The essays in the Federalist Papers, published under the pseudonym of 'Publius,' are only the most famous example of the outpouring of anonymous political writing that occurred during the ratification of the Constitution."); *id*. at 361 (Scalia, J., dissenting) ("[T]he historical evidence indicates that Founding-era Americans opposed attempts to require that anonymous authors reveal their identities on the ground that forced disclosure violated the 'freedom of the press.'").

[139] Paul Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2087 (2004) ("[P]rivacy is necessary for both "individual self-determination" and "de- mocratic deliberation.' Based in part on civic republicanism, this conception views democracy as dependent on common participatory activities, reciprocal respect, and the need for consensus about political, , , ").

[140] *See, e.g.*, Jeffrey Rosen, *The Web Means the End of Forgetting*, N.Y. TIMES, at MM30 (July 25, 2010) ("All around the world, political leaders, scholars and citizens are searching for responses to the challenge of preserving control of our identities in a digital world that never forgets. Are the most promising solutions going to be technological? Legislative? Judicial? Ethical? A result of shifting social norms and cultural expectations? Or some mix of the above?"); Mark Zuckerberg, *From Facebook, Answering Privacy Concerns with New Settings*, WASH. POST, at A19 (May 24, 2010) ("We have heard the feedback. There needs to be a simpler way to control your information. In the coming weeks, we will add privacy controls that are much simpler to use. We will also give you an easy way to turn off all third-party services."); Cecilia Kang, *Senate Online Privacy Hearing to Draw FTC, FCC Chairs, Google, Apple and Facebook*, WASH. POST: VOICES (July 23, 2010), http://voices.washingtonpost.com/posttech/2010/07/the_senate_commerce_committees.html ("Analysts said greater focus from Congress on online privacy has led Web sites and online ad networks to move toward self-regulation to fend off legislation. This self-regulation is aimed at greater disclosure on Web sites that consumers are being tracked, and an easy mechanism for opting out.").

[141] Susan Brenner, *The Privacy Privilege: Law Enforcement, Technology and the Constitution*, 7 J. TECH. L. & POL'Y (2003) 123, 191-92 ("The First Amendment protects the privacy of the identity and associates of an individual; the Fourth Amendment protects the privacy of the activities of an individual; and the Fifth Amendment protects the privacy of the thoughts of an individual.")

[142] *Id.* at 137 ("By the time the Twenty-First Century dawned . . . [t]he rise and proliferation of cybercrime raised new problems[], both with the enforcement of existing substantive laws against conduct vectored through cyberspace and also in the gathering of evidence without violating the existing privacy standards.").

removed.[143] A legal right to privacy in the United States was initially tied to physical property and one's physical person.[144] In 1890, in response to technological uses and abuses of that time,[145] (specifically "Kodakers lying in wait"[146]) Louis Brandeis and Samuel Warren conceived of a flexible,[147] yet protective, idea of an individual legal right to privacy.[148] Seventy years later, William Prosser defined and codified four tort causes of action[149] surrounding such a right.[150] The Supreme Court has noted that Prossor's codification of the privacy torts was evidence of a "strong tide" in the states valuing personal privacy.[151]

Today, Prosser's four definitive causes of action, derived from an initially fluid concept and developed at a time when privacy was defined in tandem with physical property, have proven ineffective and insufficient to the intangible digital violations of SNSs.[152] Scholarly critics claim that, although Prosser's privacy parameters were necessarily enumerated, legal institutions have

---

[143] *See* Alessandro Acquisti, *Privacy and Security of Personal Information: Economic incentives and Technological Solutions*, in THE ECONOMICS OF INFORMATION SECURITY, 179 (2004); *see generally* DANIEL SOLOVE, UNDERSTANDING PRIVACY ix ("There is no overarching conception of privacy-it must be mapped like terrain, by painstakingly studying the landscape . . . . Currently, privacy is a sweeping concept, encompassing (among other things) freedom of thought, control over one's body, solitude in one's home, control over personal information, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations.")

[144] U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects...").

[145] *See, e.g.*, Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

[146] Denis O'Brien, *Right of Privacy*, 2 COLUM. L. REV. 437, 440 (1902).

[147] Warren & Brandeis, *supra* note 145, at 293 ("Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society.").

[148] *Id.* at 198–200.

[149] William Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960) ("The law of privacy comprises four distinct kinds of invasion of four different interests of the plaintiff . . . intrusion into seclusion, disclosure of private facts, false light publicity, and appropriation of likeness.").

[150] *See id*. at 423 (1960) ("[I]t is high time that we realize what we are doing, and give some consideration to the question of where, if anywhere, we are to call a halt [in expanding the domain of privacy law]."); *see also* RESTATEMENT (SECOND) OF TORTS § 652D (1977).

[151] *See* Cox Broadcasting Corp. v. Cohn, 420 U.S. 469, 487–88 (1975).

[152] *See, e.g.*, Neil Richards & Daniel Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CALIF. L. REV. 1887, 1889 (2010); Diane L. Zimmerman, *Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort*, 68 CORNELL L. REV. 291, 362 (1983) (stating the privacy torts have "failed to become a useable and effective means of redress for plaintiffs"); Neil Richards, *The Limits of Tort Privacy*, 9 J. TELECOMM. & HIGH TECH. L. 357, 359–60 (2011) ("For better or for worse, American law currently uses tools developed in the nineteenth and mid-twentieth centuries to deal with these problems of the twenty-first.").

misunderstood their purpose, pigeonholed by precedent.[153] Trying to retrofit traditional notions of privacy protections that emphasize public exposure is misplaced for modern digital dilemmas.[154] For example, under current legal standards, liability for data breaches lies solely with the individual who placed the data, penalizing them for their choice in place rather than the individual who breached it.[155] As a scholar once summarized, "Horse law and haystack law are uneasily tolerated in the complex business of mass production and national distribution."[156]

'Privacy' originated as and has been redefined since as a reactionary concept.[157] Accordingly, throughout American history its' parameters and protections have shifted in response to economic and societal developments. For instance, the caller identification on home telephones was once shunned as violations of privacy but are now used routinely to enhance personal

---

[153] *See* Lior Strahilevitz, *Reunifying Privacy Law*, 98 CALIF. L. REV. 2007, 2034 (2010): "[T]here have been many opportunities presented for judges to address [data privacy] problems via tort rules… [I]n the majority of cases, the courts have understood themselves to be junior partners to legislators and regulators in dealing with new privacy challenges. The possibility that legislators might want to legislate has convinced the courts to stop innovating through common law. And the unwillingness of judges to modernize tort protections to deal with new challenges has prompted legislators in turn to legislate in ad hoc, often incoherent ways.").

[154] Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 481 n.18 (2006) (highlighting the ways that the legal system may fall short when it comes to protecting privacy rights in general); Joel Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?*, 44 FED. COMM. L. J. 195, 208 (1992) ("The American legal system does not contain a comprehensive set of privacy rights or principles that collectively address the acquisition, storage, transmission, use and disclosure of personal information within the business community."); Paul Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1607, 1611 (1999) ("At present, however, no successful standards, legal or otherwise, exist for limiting the collection and utilization of personal data in cyberspace."); Randall Bezanson, *The Right to Privacy Revisited: Privacy, News, and Social Change*, 80 CALIF. L. REV. 1133 (1992) (arguing society must adapt the legal concept of privacy and "embed[] [it] in a context different than external and social norms, one allowing its contours to fit the [contemporary] social and economic conditions," and advancing a privacy model rooted in "the individual's control of information" and "on an enforceable obligation of confidentiality for those possessing private information").

[155] *See generally* Alicia Solow-Niederman, *Beyond the Privacy Torts: Reinvigorating a Common Law Approach for Data Breaches*, 127 YALE L.J. F. 614 (2018).

[156] Zipporah Batshaw Wiseman, *The Limits of Vision: Karl Llewellyn and the Merchant Rules*, 100 HARV. L. REV. 465, 466 (1987).

[157] Sarah Igo, *Private Lives? Leave Me Out*, History Today (Jun. 28, 2018), www.historytoday.com/history-matters/private-lives-leave-me-out ("As in the past, we do not stop to consider what privacy consists of until it seems – just like that – to fall victim to unimagined breaches. And, as in the 19th century, when wiretapping and candid photography were new, today's technologies of data-harvesting and scraping are already transforming our beliefs about the borders of our private selves.").

privacy.[158] Although America has redefined privacy protections to meet the needs of individual issues of the times, the aims of individual determinism and democratic deliberation have always been at the core of its' meaning.[159]

The paramaters of a modern definition of personal privacy should, at a minimum, encompass an individual's right to control their identity which is now inextricably tied to their digital data.[160] Personal *control* over one's identity is fundamental to individual liberty in America.[161] It is only once an individual is empowered to take responsibility of their self can one engage in democratic deliberation through *consent.*[162] Justice Story conceptualized of consent as "an act of reason, accompanied with deliberation, the mind weighing, as in a balance the good or

---

[158] See generally, Tene & Polonetsky, *supra* note 65.

[159] *See, e.g.* Lee Bygrave & Kamiel Koelman, *Privacy, Data Protection and Copyright: Their Interaction in the Context of Electronic Copyright Management Systems*, in COPYRIGHT AND ELECTRONIC COMMERCE: LEGAL ASPECTS OF ELECTRONIC COPYRIGHT MANAGEMENT 59, 64-65 (2000); *see also* Moore v. Regents of Univ. of Calif., 793 P.2d 479 (Cal. 1990); Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373 (2000); Charles Fried, *Privacy*, 77 YALE L.J. 475 (1968); Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049 (2000).

[160] *See* ALAN WESTIN, PRIVACY AND FREEDOM, 7 (1968) (Writing that "Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."); Jed Rubenfeld, *The Right of Privacy*, 102 HARV. L. REV. 737, 805 (1989) (noting that "the right to privacy exists because democracy must impose limits on the extent of control and direction that the state exercises over the day-to-day conduct of individual lives"); *See generally* Jules Polonetsky & Omer Tene, *Privacy and Big Data: Making Ends Meet*, 66 STAN. L. REV. ONLINE (2013) (arguing control of data must ultimately rest with the individual).

[161] Mark Andrus, *The New Oil: The Right to Control One's Identity in Light of the Commoditization of the Individual*, AM. BAR ASS'N (September 28, 2017) www.americanbar.org/groups/business_law/publications/blt/2017/09/06_andrus/.

[162] A number of privacy law scholars have documented how the imoprtance of consent is currently impractically conditioned as an all-or-nothing proposition for users. *See, e.g.*, Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, WASH. U. L. REV. (2019) ("Consent transforms the moral landscape . . . It reinforces fundamental cultural notions of autonomy and choice."); Elizabeth Edenberg & Meg Jones, *Analyzing the Legal Roots and Moral Core of Digital Consent*, 21 NEW MEDIA & SOC'Y 1804 (2019); Meg Leta Jones, *The Development of Consent to Computing*, IEEE ANNALS OF THE HISTORY OF COMPUTING 1 (2019); Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006); NANCY KIM, WRAP CONTRACTS (2013); MARGARET RADIN, BOILERPLATE: THE FINE PRINT, VANISHING RIGHTS, AND THE RULE OF LAW (2012); Andrea M. Matwyshyn, *Technoconsen(t)sus*, 85 WASH. U. L. REV. 529 (2007); Scott Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security & Consent*, 93 TEX. L. REV. 85 (2014).

evil on each side."[163] Thus, consent naturally portends with control over one's identity and is necessarily integral to a modern reconception of the reactionary concept of 'privacy'. Tellingly, in a recent Congressional inquiry regarding abuse and misuse of personal data, the chief executive officer of Facebook, Mark Zuckerburg, looking to escape the potential of federal regulatory oversight, went out of his way to say more than one thousand times over the course of the hearing that he is working to ensure "Facebook puts users in 'control'."[164]

B. The Institutions

The amorphous nature of American personal privacy in the digital age has translated into a patchwork of 'protections'[165] that are often in conflict with other regulations and remedies[166] and permits ample abuse. For example, in the first six months of 2019, there have been 3,800 publicly disclosed breaches of personal data, totaling an astonishing 4.1 billion individual records.[167]

---

[163] 1 Joseph Story, Commentaries on Equity Jurisprudence § 222 (1835).

[164] *Facebook: Transparency and Use of Consumer Data: Hearing Before the H. Comm. on Energy & Commerce*, 115th Cong. 2 (2018) (statement of Mark Zuckerberg) www.energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Testimony-Zuckerberg-FC-Hrg-on-FacebookTransparency-and-Use-of-ConsumerData-2018-04-11.pdf; *see also*, Mark Zuckerberg, *A Privacy-Focused Vision for Social Networking*, FACEBOOK (Mar. 6, 2019), www.facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634/ ("This privacy-focused platform will be built around several principles: People should have simple, intimate places where they have clear control over who can communicate with them and confidence that no one else can access what they share."); Dan Fletcher, *Facebook Mania: Privacy Changes for Nearly 500 Million*, TIME (May 20, 2010), www.content.time.com/time/magazine/article/0,9171,1990798-4,00.html ("The way that people think about privacy is changing a bit. . .What people want isn't complete privacy. It isn't that they want secrecy. It's that they want control over what they share and what they don't."); Anita Balakrishnan et al., *Facebook CEO Mark Zuckerberg's statements on privacy, 2003-2018*, CNBC (Apr. 9, 2018), www.cnbc.com/2018/03/21/facebook-ceo-mark-zuckerbergs-statements-on-privacy-2003-2018.html ("When I built the first version of Facebook, almost nobody I knew wanted a public page on the internet. That seemed scary. But as long as they could make their page private, they felt safe sharing with their friends online. Control was key.").

[165] Woodrow Hartzog, *Privacy and Terms of Use.*, *in* SOCIAL MEDIA AND THE LAW 50 (2d ed. 2017).

[166] *See, e.g.*, David Ruiz, *US Congress Proposes Comprehensive Federal Data Privacy Legislation—Finally*, Malwarebytes Labs (Mar. 7, 2019), www.blog.malwarebytes.com/security-world/privacy-security-world/2019/03/what-congress-means-when-it-talks-about-data-privacy-legislation ("Businesses are expected to comply with data privacy laws based on the data's type. Law enforcement agencies and the intelligence community, on the other hand, are expected to comply with a different framework that sometimes separates data based on "content" and "non-content.")

[167] RISK BASED SECURITY, 2019 MIDYEAR QUICKVIEW DATA BREACH REPORT (Nov. 2019), https://pages.riskbasedsecurity.com/2019-midyear-data-breach-quickview-report.

Conversely, less than 1% of cybersecurity breaches were successfully enforced last year due the inability to identify the hacker source.[168]

The current paradoxical dichotomy of providing privacy for digital abusers, but not innocent users,[169] stems from the United States' inception of the Internet when the government affirmatively chose not to implement digital security measures.[170] Instead, government institutions have been left to their respective devices[171] to retrofit legal standards[172] that are often inadequate deterrents for modern digital deceptions.[173] In considering effectuating a meaningful privacy paradigm shift, each branch of government offers particular compententcies in effectuating such,[174] and there is much scholarly debate as to the realitive efficacy of each.[175]

---

[168] Mieke Eoyang et al., *To Catch a Hacker: Toward a Comprehensive Strategy to Identify, Pursue, and Punish Malicious Cyber Actors* (Cyber Enforcement Initiative., Third Way), Oct. 29, 2018.

[169] *See* Laurie Baughman, *Friend Request or Foe?*, 19 WIDENER L.J. 933, 944 (2010) ("[SNS] run on the honor system. The sites do not check into whether a user who creates a profile is in fact a real person, so the creation of a fake profile is as easy as the creation of a real profile. A fake profile may allow an abuser to access the site of a victim or victim's family member, when an authentic profile would act as a red flag.") (footnotes omitted).

[170] *See* Greg Allen & Taniel Chan, *Artificial Intelligence and National Security*, BELFER CTR. FOR SCI. AND INT'L AFF. (Jul. 2017).

[171] Debra Cassens Weiss, *Does Fourth Amendment Protect Computer Data? Scalia Says It's a Really Good Question*, AM. BAR ASS'N (Mar. 24, 2014) www.abajournal.com/news/article/asked_about_nsa_stuff_scalia_says_conversations_arent_protected_by_fourth_a.

[172] Carpenter v. United States, 138 S. Ct. 2206, 2209 (2018) ("The digital data at issue—personal location information maintained by a third party—does not fit neatly under existing precedents . . . .")

[173] ANDREA WECKERLE, CIVILITY IN THE DIGITAL AGE 251 (2013) ("Privacy laws, such as the Electronic Communications Privacy Act, are considered woefully antiquated. For example, email older than 180 days receives no privacy protection, and, under current law, it is possible to access these materials without a judge's permission and simply with an administrative subpoena, which many privacy experts find disturbing.")

[174] For an in-depth discussion on each branch's strengths and weakness, *see* Matthew Scherer, *Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies*, 29 HARV. J.L. & TECH. 354 (2016).

[175] Connie Powell, *"You Already Have Zero Privacy. Get Over It!,"* 31 PACE L. REV. 146, 179–81 (2011) (arguing courts should extend the common law privacy causes of action to cover disclosure and commercialization of personal information); Jonathan Frieden et al., *Putting the Genie Back in the Bottle: Leveraging Private Enforcement to Improve Internet Privacy*, 37 WM. MITCHELL L. REV. 1722–25 (2011) (stating courts should resolve privacy controversies and Congress should propose new legislation that establishes additional privacy causes of action); FREDERICK LANE, AMERICAN PRIVACY: THE 400-YEAR HISTORY OF OUR MOST CONTESTED RIGHT 258 (2011) (disagreeing with a focus on court action and, instead, stressing the need for a new federal administrative agency with a broad mandate to define and prosecute privacy infringements); Catherine Schmierer, *Better Late than Never: How the Online Advertising Industry's Response to Proposed Privacy Legislation Eliminates the Need for Regulation*, 17 RICH. J.L. & TECH. 56–57 (advocating industry self-regulation is preferable anytime rapidly

1. The FTC

The United States has always prioritized the collective public good stemming from the free flow of information over individual privacy.[176] In the 1970s, the United States, along with the United Kingdom, created a framework of "fair information practice principles" ("FIPPs")[177] which encapsulated and promoted this priority of the collective good. Created as a model for Western nations to adopt and guide their respective data protection laws, FIPPs centered on four core principles: "(1) defined obligations that limited the use of personal data; (2) transparent processing systems; (3) limited procedural and substantive rights; and (4) external oversight."[178] Accordingly, in the early days of the Internet in the 1990s, the Federal Trade Commission ("FTC"), encouraged American businesses to adopt and publish online privacy policies in line with these FIPPs.[179] The United States even embodied the FIPPs in other statutory regulations outside the digital realm.[180]

As the FIPPs were incorporated around the world alongside the spread of the Internet, the FTC abruptly diverted away from the core principles. In 1998, the FTC revised their focal priorities and declared the primacy of "notice," or procedural rquirements, as the "most fundamental principle," thereby abandoning the core commitments to substantive personal data protections.[181] The impact of the United States' ideological departure from the FIPPs has reverberated into deep

developing technology is involved); Lauren Gelman, *Privacy, Free Speech, and "Blurry-Edged" Social Networks*, 50 B.C. L. REV. 1315, 1342 (2009) (suggesting a system where people tag their data with labels indicating permissible uses).

[176] Westin, *supra* note 188; Margaret O'Mara, *The End of Privacy Began in the 1960s*, N. Y. TIMES, at A31 (Dec. 6, 2018).

[177] ORG. FOR ECON. CO-OP. & DEV., GUIDELINES ON PROTECT. OF PRIV'Y & TRANSBORDER FLOWS OF PERS. DATA (1981).

[178] Schwartz, *supra* note 139, at 1614.

[179] *See, e.g.*, FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS 7 (1998).

[180] *See, e.g.*, Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681x (2018) (consumer financial information); 45 C.F.R. §§160, 162, 164 (patient health data privacy).

[181] *Privacy Online*, *supra* note 179.

divides to this day.[182] For example, the European Union has insisted on the development and use of "safe harbor" procedures,[183] which have heightened levels of privacy protection, in all data commerce with the United States today.[184]

The only American federal body authorized to oversee and administer personal data privacy regulations today is the FTC. [185] In line with the revised, FIPPs-free focus, and aside from a limited set of special circumstances,[186] the agency's jurisdiction is predicated on affirmative commercial misrepresentative practices,[187] such as explicitly deceptive spam e-mails, misleading instructions, and fake advertisements.[188] Under these FTC guidelines, SNSs' neuroscientific driven data collection practices have, thusfar, been shielded,[189] as long as somewhere on their

---

[182] *See generally* Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 92 (2001); *see also, e.g.,* O'Mara, *supra* note 197 ("This was a contrast to Western Europe, where privacy was something to be carefully protected, and therefore treated with a far more robust regulatory approach. In being so relentlessly focused on government's use and abuse of data, Congress paid little attention to what private industry was doing. American companies remained free to gather data on people who use their products.").

[183] EU-U.S. & Swiss-U.S. Privacy Shield.

[184] For more on this fracture and Europe's relative success in continuing to follow the FIPPs, *see, e.g*., Paul Schwartz, *European Data Protection Law and Restrictions on International Data Flows*, 80 IOWA L. REV. 471 (1995); David Scheer, *Europe's New High-Tech Role: Playing Privacy Cop to World*, WALL ST. J., at A1 (Oct. 10, 2003); Adam Satariano, *New Privacy Law, Makes Europe World's Leading Tech Watchdog*, N. Y. TIMES, at A1 (May 25, 2018).

[185] FTC Act, 15 U.S.C. § 45 *et seq.* (2018) (empowering the agency broadly to enforce unfair or deceptive consumer data practices and to enforce federal privacy and data regulations).

[186] Specific limited jurisdictional authority was extended to the FTC in order to police privacy practices by the Children's Online Privacy Protection Act of 1998 ("COPPA"), 15 U.S.C. §§ 6501-6506 (2018); *see also* FED. TRADE COMM'N, CHILDREN'S PRIVACY (2018*)* www.ftc.gov/tips-advice/business-center/privacy-and-security/children %27s-privacy.

[187] *See, e.g.,* FED. TRADE COMM, *5 Billion Facebook Settlement: Record-Breaking and History-Making* (Jul. 24, 2019), www.ftc.gov/news-events/blogs/business-blog/2019/07/ftcs-5-billion-facebook-settlement-record-breakinghistory; Thompson Medical Co. v. FTC, 791 F.2d 189, 196 (D.C. Cir. 1986); *In re* International Harvester Co., 104 F.T.C. 949, 1041 (1984); PETER C. WARD, FEDERAL TRADE COMMISSION: LAW, PRACTICE, AND PROCEDURE § 5.04[2] (2002).

[188] *See* FED. TRADE COMM'N, PRIVACY & DATA SECURITY UPDATE (2018), https://www.ftc.gov/reports/privacy-data-security-update-2018.

[189] *In re* Facebook, Inc., Consumer Privacy User Profile Litig., MDL No. 2843 (N.D. Cal. Sep. 9, 2019) (faulting Facebook for treating privacy as an "all-or-nothing" proposition, "sharing information with your social media friends does not categorically eliminate your privacy interest in that information.")

platform some semblance of a privacy policy exists.[190]

2. Congress

Last year the Senate's Commerce and Judiciary committees called Facebook Chief Executive Officer (CEO) Mark Zuckerberg to testify to explain Facebook's privacy policies in light of the mass Russian meddling on his network.[191] Senator Orrin Hatch began by earnestly asking Mr. Zuckerberg, "[So], how do you sustain a business model in which users don't pay for your service?"[192] The CEO stifled a laugh, smirked, and replied, "Senator, we run ads."[193]

Like the courts, legislative bodies have been slow to respond to rapid digital advancements.[194] While there have been numerous Congressional hearings on digital data privacy this year,[195] neither the House of Representatives nor the Senate have enacted any comprehensive data protection legislation. Currently, Congress has set forth a sectorial statutory patchwork

---

[190] *See* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (Mar. 2012); Neil Richards & Woodrow Hartzog, *Taking Trust Seriously In Privacy Law*, 19 STAN. L. REV 431 (2016); Woodrow Hartzog, *The New Price to Play: Are Passive Online Media Users Bound By Terms of Use?*, 15 COMM. L. & POL'Y 405 (2010).

[191] Confessore et al., *supra* note 1.

[192] *Facebook, Social Media Privacy, and the Use and Abuse of Data, Hearing* Before the H. Comm. on Commerce, Sci., & Trans., 116th Cong. 1 (Apr. 10, 2018) (testimony of Mark Zuckerberg).

[193] *Mark Zuckerberg's Senate Hearing*, WASH. POST (Apr. 10, 2018), www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/.

[194] In 2016, the first Congressional hearing regarding A.I. was conducted, more than half a century after the military and sciences began developing such technology, *see The Dawn of Artificial Intelligence, Hearing Before S. Comm. on Commerce, Science & Transp.*, 115th Cong. 2 (2016).

[195] *See, e.g., Policy Principles for a Federal Data Privacy Framework in the United States, Hearing Before S. Comm. on Commerce, Science, and Transp.*, 116th Cong. 1 (2019); *Protecting Consumer Privacy in the Era of Big Data, Hearing Before Subcomm. on Cons. Protection & Commerce*, 116th Cong. 1 (2019); *Consumer Data Privacy: Examining Lessons from the European Union's Data Protection Regulation and the California Consumer Privacy Act, Hearing Before S. Comm. on Commerce, Sci., and Transp.*, 115th Cong. 2 (2018); *Examining Safeguards for Consumer Data Privacy, Hearing Before S. Comm. on Commerce, Sci., and Transp.*, 115th Cong. 2 (2018); *Examining the Current Data Security and Breach Regulatory Notification Regime, Hearing Before Subcomm. on Fin. Inst. & Consumer Credit*, 115th Cong. 1 (2018).

addressing data privacy statutes,[196] some of which include a private right of action.[197] Following September 11, 2001, personal privacy concerns[198] have, again, taken a back seat to national security.[199] While state legislatures have taken to slowly passing statutory regulations addressing personal data privacy,[200] the effectiveness of their siloed protections is questionable in a boundary-less digital world.

New bipartisan calls for federal personal SNSs data protections following the 2016 election have increased,[201] even prompting SNSs to preemptively ask for them in hopes of staving off more dense regulatory measures.[202] Regardless, instead of taking a proactive prescriptive approach, the

---

[196] *See, e.g.*, Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, H.R. 3103, 104th Cong. (codified in numerous different places, regulating protected health information in the health sector); Children's Online Privacy and Protection Act of 1998, 15 U.S.C. § 6501, *et seq.* (regulating data of minors); Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (regulating data contained education records); Gramm-Leach-Bliley Act, 15 U.S.C. § 6801, *et seq*.; Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.* (regulating the collection and use of consumer credit report data).

[197] *See, e.g.*, Telephone Consumer Protection Act, 47 U.S.C. § 227(b); Video Privacy Protection Act, 18 U.S.C. § 2710(C); Cable Privacy Act, 47 U.S.C. § 5I(f); Electronic Communication Privacy Act, 18 U.S.C. § 2707.

[198] *See* Part.II.B.1.

[199] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism ("USA PATRIOT ACT") Act of 2001, Pub. L. No. 107-56, H.R. 3162, 107th Cong.

[200] *See, e.g.*, Vermont Data Broker Regulation, 9 V.S.A. §§ 2430, 2433, 2446, 2447 (2018) (regulating data brokers); California Consumer Privacy Act of 2018 (SB-1121) (creating the strongest personal privacy data rights in the world). Also, several Senators running for President this year have proposed similar national legislation, *see e.g.*, Diane Bartz, "U.S. Senators Want Social Media Users to Be Able to Take Their Data with Them." REUTERS (Oct. 22, 2019), www.reuters.com/article/us-tech-antitrust-congress/u-s-senators-want-social-media-users-to-be-able-to-take-their-data-with-them-idUSKBN1X112C; Marty Swant, *Andrew Yang Proposes Digital Data Should Be Treated Like A Property Right*, FORBES, www.forbes.com/sites/martyswant/2019/10/01/andrew-yang-proposes-digital-data-should-be-treated-like-a-property-right/ (detailing regulatory proposals from presidential candidates Senators Amy Klobuchar and Elizabeth Warren, as well as Andrew Yang, that provide personal privacy protections over SNSs data).

[201] Pamela Maclean, *Google Resists Becoming Digital 'Town Square' in Censorship Spat*, BLOOMBERG (Mar. 15, 2018), www.bloomberg.com/news/articles/2018-03-15/google-resists-becoming-digital-town-square-in-censorship-spat ("Silicon Valley's social media giants are under attack from both the left and the right for not doing enough").

[202] *See, e.g.*, Ben Kochman, T*ech Giants Want Uniform Privacy Law, But No GDPR*, Law360 (Sept. 26, 2018), www.law360.com/articles/1086064 ("Representatives from Google LLC, Amazon.com Inc., Apple Inc., Twitter Inc., AT&T Inc. and Charter Communications Inc. all said they would support some sort of privacy law that would give consumers more control over the way in which their data is used."); Harper Neidig, A*dvocates Draw Battle Lines over National Privacy Law*, The Hill (Nov. 13, 2018), www.thehill.com/policy/technology/416341-advocates-draw-battle-lines-over-national-privacy-law (reporting thirty-four public interest groups are now advocating for comprehensive federal data privacy legislation).

Trump Administration has double-downed on an institutional reactionary approach rather than develop preventive practices.[203] In 2017, President Trump signed a congressional resolution to repeal protective measures enacted before his election that would have prevented internet service providers from collecting, mining, and selling customer information without permission.[204] In line with President Trump's change in course, his latest Attorney General, Robert Barr, demanded SNSs, such as Facebook, develop technology that gives the government access to *more* of users' private online communications otherwise he would ensure punitive legislative measures would be "on the way."[205]

3. The Judiciary

Absent explicit textual command, the courts have interpreted the United States Constitution as protecting personal rights to decisional and informational privacy.[206] Attempts to establish whether such Constitutional protections extend to personal digital data have failed at their inception given the standing requirement,[207] which requires a particularized, concrete, and imminent injury.[208] The intangible nature of digital data deceptions has made it nearly impossible

---

[203] *Developing the Administration's Approach to Consumer Privacy*, NAT'L TELECOMM. & INFO. ADMIN., U.S. DEPT. OF COMM., 83 Fed. Reg. 48600, 48601 (Sept. 26, 2018) ("The Administration is instead proposing that discussion of consumer privacy in the United States refocus on the outcomes of organizational practices, rather than on dictating what those practices should be.")

[204] Steve Lohr, *Trump Completes Repeal of Internet Privacy Rules*, N.Y. TIMES, at B3 (Apr. 4, 2017).

[205] William Barr. Attorney General, U.S. Dept. of J., Keynote Address at Fordham University Int'l Conf. on Cyber Sec. (July 23, 2019).

[206] *See, e.g.*, U.S. CONST. amend. IV(containing the only explicit textual reference to information privacy); For decisional privacy reflected in jurisprudence, *see e.g.*, Griswold v. Conn., 381 U.S. 479 (1965) (marital privacy); Roe v. Wade, 410 U.S. 113 (1973) (right to abortion); *see also* Whalen v. Roe, 429 U.S. 589 (1977) (identifying two different privacy interests which may be constitutionally protected: the interest of controlling the disclosure of personal matters and the interest in being able to make certain personal decisions free from government influence).

[207] *See* Clapper v. Amnesty Int'l, 568 U.S. 398, 409-10 (2013) (stating that imminence requires the alleged injury be "certainly impending" to constitute injury-in-fact, speculation and assumptions cannot be the basis.); Warth v. Seldin, 422 U.S. 490, 498–99 (1975) ("In its constitutional dimension, standing imports justiciability: whether the plaintiff has made out a 'case or controversy' between himself and the defendant within the meaning of Art. III. This is the threshold question in every federal case, determining power of the court to entertain.")

[208] U.S. CONST. Art. III.

for plaintiffs to successfully direct injury[209] and subsequent, tangible harms.[210] Conversely, in personal data adjudications governed by specific statutory protections that provides for a private cause of action, lower courts have generally conferred standing.[211]

The first Supreme Court case related to personal protections on the Internet was on First Amendment grounds,[212] leaving lower courts[213] and scholars[214] to speculate the significance of prioritizing free speech over or even exclusive to a common law right to personal digital privacy. Two decades later, Justice Kennedy stated that, "While in the past there may have been difficulty in identifying the most important places (in a spatial sense) for the exchange of views, today the

---

[209] *See, e.g.*, Beck v. McDonald, 848 F.3d 262, 272-76 (4th Cir. 2017) (relying on *Clapper*, dismissing a suit regarding two data breaches as too speculative); In re OPM Data Security Breach Litig., 266 F. Supp. 3d 1,35 (D.D.C. 2017) (acknowledging a data breach exposed sensitive information which could form the "building blocks" of identity theft, but dismissing as too attenuated); *C.f.* In re Zappos.com, Inc., 888 F.3d 1020, 1025 (9th Cir. 2018) (holding that "increased risk of future identity theft" could give rise to standing in data breach case following *Clapper*); Attias v. Carefirst, Inc., 865 F.3d 620, 628-29 (D.C. Cir. 2017) (holding plaintiffs plausibly alleged "substantial risk" of identity theft in data breach case where "[n]o long sequence of uncertain contingencies involving multiple independent actors has to occur before the plaintiffs in this case will suffer any harm").

[210] *See* Robins v. Spokeo, 867 F.3d 1108, 1118 (9th Cir. 2017), *cert. denied* Spokeo v. Robins, 138 S. Ct. 931, 1549 (2018) (remanding because plaintiff needed to demonstrate a concrete injury separate from a particularized injury, meaning show that their injury "actually exist[ed]."") Note: On remand, the lower court determined plaintiff's alleged injury was both concrete and particularized, and thus, had standing.

[211] *See, e.g.*, Eichenberger v. ESPN, 876 F.3d 979, 983–84 (9th Cir. 2017) (asserting standing for violations of the right to privacy under the Video Privacy Protection Act); Susinno v. Work Out World, Inc., 862 F.3d 346, 352 (3d Cir. 2017) (holding customer's receipt of unsolicited calls in violation of the Telephone Consumer Protection Act was sufficiently concrete); *In re* Horizon Healthcare Services Inc. Data Breach Litig., 846 F.3d 625, 640–41 (3d Cir. 2017) ("So the Plaintiffs here... allege [] the unauthorized dissemination of their own private information—the very injury that FCRA is intended to prevent. There is a de facto injury that satisfies the concreteness requirement for standing.").

[212] Reno v. ACLU, 521 U.S. 844, 870 (1997) (explaining the importance of "provid[ing] the Internet with the broadest possible First Amendment protection").

[213] *See, e.g.*, Birnbaum v. U.S., 588 F.2d 319, 326 (2d Cir. 1978) (describing the distinction between common law and constitutional privacy claims); Drake v. Covington County Bd. of Educ., 371 F. Supp. 974, 980 (M.D. Ala. 1974) (Johnson, C.J., concurring) (stating that the Warren-Brandeis right of privacy is a creature of state law and is not constitutionally based); Mimms v. Philadelphia Newspapers, Inc. 352 F. Supp. 862, 865 n. 5 (E. D. Pa. 1972) (distinguishing right of privacy from constitutional cases); Paul v. Davis, 424 U.S. 693, 713 (1976) (constitutional right to privacy limited to unreasonable government searches or interference with matters relating to family and reproduction).

[214] *See e.g.*, Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049 (2000) (opining "the privacy torts may be of limited practical and doctrinal utility in a society that also prioritizes freedom of speech"); Jack Balkin, *Free Speech is a Triangle*, 18 COLUM. L. REV. 2011 (2012) (writing "at least until the courts begin to treat cyberspaces differently from other public fora—applying First Amendment law would cripple [SNSs'] abilities to impose civility norms").

answer is clear. It is cyberspace—the 'vast democratic forums of the Internet' in general, and social media in particular."[215] Again, the lower courts and scholars quickly interpreted this statement as the Court's signaling the preeminence of free speech on the Internet over all else.[216]

These, quick interpretations of the Supreme Court are fundamentally flawed and indicative of the need for a uniform national law protecting personal digital privacy. The lower courts and scholars' logic mistakes content, which is digital speech, with individuals actions on SNSs, such as posting, liking, and commenting, which is collected as digital data. In other words, content is what users *say*, data is what they *do.* are indicative of the necessity for a uniform national law protecting personal data privacy.

III. THE PROPERTIZATION OF PERSONAL SOCIAL MEDIA DATA

A complex issue requires an innovative, nuanced solution and sincethe New Deal, some regulatory measures have been driven by shifting societal considerations, not constitutionally constrainted.[217] Given the integral role neuroscience plays in the symbiotic digital ecosystem between the individual and SNSs, a modern solution must necessarily account for the science, as well. Accordingly, casting personal digital data as personal property in American common law most accurately reflects how both individuals already implicitly view their online and offline actions as one in the same and SNSs' commodification of individuals allows them to profit. Section

---

[215] Packingham v. North Carolina, 137 S.Ct. 1730, 1735 (2017).

[216] *See, e.g.,* Sorrell v. IMS Health Inc., 564 U.S. 552, 570 (2011) ("[T]he creation and dissemination of information are speech within the meaning of the First Amendment."); *see also* Jane Bambauer, *Is Data Speech?*, 66 STAN. L. REV. 57, 71–72 (2014) (arguing that data should be treated as speech for purposes of the First Amendment); *cf.* Los Angeles Police Dept. v. United Reporting Pub. Corp., 528 U.S. 32 (1999) (characterizing personal information as a "thing in commerce"); Reno v. Condon, 528 U.S. 141 (2000) (holding sale of personal information is not being treated as speech).

[217] *See generally* Neil Richards, *Why Data Privacy Law Is (Mostly) Constitutional*, 56 WM. & MARY L. REV. 1501 (2015) (arguing the pervasiveness of data in society today means we must necessarily conceive its protections under commercial regulation principles not constitutional concepts like freedom of speech).

A defines and details the idea of SNSs data as personal property. Section B explains the resulting role SNSs would play in such a shift as information bailees.

A. The Idea

The economic outlook[218] and scientific studies[219] already consider personal digital data as property. American legal institutions, on the other hand, have yet to align effectively with this reality, as previously discussed. The importance of defining and demarcating digital data as personal *property* allows for individuals, institutions, and SNSs, alike, to develop policies and protocols reflective of fundamentally equitable values.[220]

The traditional definition of a 'property' right is an "interest. . . that is enforceable against the world."[221] Reconceptualizing digital data as a personal right against the world, aligns with the previously discussed modern reevaluation of privacy consisting of control and consent,[222] best

---

[218] Palmer, *supra* note 129.

[219] Karolina Sylwester & Matthew Purver, *Twitter Language Use Reflects Psychological Differences between Democrats and Republicans*, 10 PLOS ONE (2015) (discovering that the psychological disparities among people with differing political orientations through individual word use on Twitter was resonant with previous research; liberals tend to place more emphasis on uniqueness and use more swear words, anxiety- and feeling-related words while conservatives value group association and their tweets contain more achievement and religion-related words); Danah Boyd, *Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life*, MACARTHUR FOUNDATION SERIES ON DIGITAL LEARNING –YOUTH, IDENTITY, AND DIGITAL MEDIA VOLUME 15 119, 129 (2008) ("Because of the intricate connection between offline and online social worlds, the audience that teens envision online is connected to their social world offline, or to their hopes about the possible alternatives online."); Dar Meshi et al., *The Emerging Neuroscience of Social Media*, 19 TRENDS IN COGN. SCI. 771 (2015) ("While the neural systems supporting these social cognitive processes have been studied extensively in the offline world, the online social media is comparatively new. However, experts continue to conclude that the digital world often mimics the offline social world and interactions within this online social network parallel offline social interactions."). *See generally* CHRISTINE HINE, VIRTUAL ETHNOGRAPHY (2000); Malene Charlottte Larsen, *Perspectives on Online Social Networking*, 35 SOC. COMP. MAG. (2007)..

[220] Samuelson, *supra* note 184, at 1170–71 ("[A] serious impediment to a comprehensive approach [to privacy] in the U.S. is the lack of clarity… about the nature of the interest that individuals have in information about themselves: Is it a commodity interest, a consumer protection interest, a personal dignity interest, a civil right interest, all of the above, or no interest at all?").

[221] Paul Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2059-51 (2004) (explaining this right against the world does not mean "Blackstonian despotism over the res, but rather a bundle of related interests relating to the res.")

[222] *See infra* Part II.A.

redefined relative to data-as-property as the individual's ability and right to decide on and demarcate boundaries (if any) around their property.[223] A propertization of individuals personal data would include the common law rights that run with property,[224] including transferability and alienability.[225] Propertization of personal data also reaffirms the Framer's fundamental aims of democratic deliberation and indivual determinism by reallocating property to its' rightful owner as it empowers and encourages such exchanges. [226]

America has a long history of defining and regulating privacy in tandem with property.[227], In fact, some courts have already indicated an inclination to apply property principles to digital intangibles.[228] While some scholars are sharply divided on the efficacy of treating digital data as property believing it could lead to a slippery slope of black-market data tradingm[229] other would

---

[223] Julie Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373 (2000) (defining "privacy as shorthand for breathing room to engage in the processes of boundary management that enable and constitute self-development.").

[224] Henry Hansmann & Reinier Kraakman, *Property, Contract, and Verification: The Numerus Clausus Problem and the Divisibility of Rights*, J. LEG. STUD. S373 (2002) (conceptualizing information as a property right that "runs with the asset").

[225] Thomas Merrill, *The Property Strategy*, 160 U. PA. L. REV. 2061, 2079 (2012) ("Property law's hallmark is the right of alienation—the voluntary right to agree to transfer one's property, real or personal—to another.").

[226] Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules and Inalienability: One View of the Cathedral*, HARV. L. REV. 1092 (1972) (arguing that in a property regime "the value of the entitlement is agreed upon by the seller.")

[227] *See infra*, Part II.B.

[228] Salonclick LLC v. Superego Mgmt. LLC,. 2555 (S.D.N.Y. May 8, 2017) (acknowledging SNSs have a possessory interest in their domain names); Sprinkler Warehouse, Inc. v. Systematic Rain, Inc., 880 N.W.2d 16, 23 (Minn. 2016) (holding an Internet domain is intangible personal property); Integrated Direct Mktg., LLC v. May, 495 S.W.3d 73, 76 (Ark. 2016) (holding intangible property, such as electronic data, can be converted); In re CTLI, LLC, 528 B.R. 359 (Bankr. S.D. Tex. 2015) (holding SNSs accounts are property interests under the bankruptcy code, and therefore reversion applies).

[229] *See, e.g.*, Julie Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1391 (2000) ("Recognizing property rights in personally-identified data risks enabling more, not less, trade and producing less, not more, privacy."); Anita Allen, *Coercing Privacy*, 40 WM. & MARY L. REV. 723, 750–57 (1999); Simon Davies, *Re-Engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity*, *in* TECH. AND PRIV. 143, 160 (Philip Agre & Marc Rotenberg eds., 1997); Mark Lemley, *Private Property: A Comment on Professor Samuelson's Contribution*, 52 STAN. L. REV 1545, 1551 (2000) ("from a privacy perspective, an intellectual property right that is regularly signed away may turn out to be less protection than we want to give individuals."); Rotenberg, *supra* note 204, at 92–97; Samuelson, *supra* note 184, at 1443.

like to take the idea to the other extreme, disregarding privacy concerns, altogether.[230]

B. The Information Bailees

Recasting the role of SNSs as information bailess best reflects the reality of the current digital ecosystem. SNSs' rely on and are driven by individuals engaging and thereby creating the personal data which the platforms, in turn, commodify. In creating and harvesting this digital dependence, SNSs should have, and arguably already do, the role and responsibilities of bailees.[231]

Revising the roles of SNSs as fiduciaries recalibrates the power dynamics of their relationship with users. Today, SNSs implicitly encourage users to trust them with personal information, so implementing a corresponding duty of confidentiality and care on SNSs is not such a stretch. The current implicit contractual relationship between SNSs and users[232] is is asymmetrically disadvantageous to individuals. Simnilar to personal physicians and lawyers, SNSs relationship with users presupposes contractual duties.[233]

---

[230] *See, e.g.*, LESSIG, *supra* note 61, at 143–63; Patricia Mell, *Seeking Shade in a Land of Perpetual Sunlight*, 11 BERKELEY TECH. L.J. 26, 26–41 (1996); Richard Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381, 2385 (1995–1996); *Developments in the Law — The Law of Cyberspace*, 112 HARV. L. REV. 1574, 1634–49 (1999); Kenneth Laudon, *Markets and Privacy*, 39 COMM. OF ACM 92, 92 (1996).

[231] Jack Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. Davis L. Rev. 1183, 1209 (2016)("An information fiduciary is a person or business who, because of their relationship with another, has taken on special duties with respect to the information they obtain in the course of the relationship."); Jack Balkin, *The Three Laws of Robotics in the Age of Big Data*, 78 OHIO ST. L.J. (2017)("When fiduciaries collect and process information about their clients, . . . [t]hey are information fiduciaries.").

[232] *See, e.g.*, *Terms of Service*, Facebook (Jul. 31, 2019), www.facebook.com/terms ("We cannot predict when issues might arise with our Products. Accordingly, our liability shall be limited to the fullest extent permitted by applicable law, and under no circumstance will we be liable to you for any lost profits, revenues, information, or data, or consequential, special, indirect, exemplary, punitive, or incidental damages arising out of or related to these Terms..."); *Terms of Service*, Twitter www.twitter.com/content/twitter-com/legal/en/tos.html (May 25, 2018) ("in no event shall the aggregate liability of the twitter entities exceed the greater of one hundred U.S. dollars"); *Terms of Use*, Instagram www.help.instagram.com/581066165581870 ("You agree that we won't be responsible for any lost profits, revenues, information, or data, or consequential, special, indirect, exemplary, punitive, or incidental damages arising out of or related to these Terms, even if we know they are possible.").

[233] Balkin, *supra* note 230.

CONCLUSION

Recasting personal data as property and revising the role of SNSs as bailess avoids the prickly path of complex constitutional considerations[234] and accurately accounts for encapsulates the science already existing in their symbiotic relationship. To further entice SNSs to shift their role and reshape their relationship with users, some scholars have proposed regulations affording the platforms greater constitutional protections, particularly preempting the patchwork of state privacy laws.[235]

[234] *See, e.g.*, Lowe v. SEC, 472 U.S. 181, 210–11 (1985) (distinguishing between regulation of public and private investment advisors in order to prevent "fraud, deception, or overreaching"); ROBERT POST, DEMOCRACY, EXPERTISE, AND ACADEMIC FREEDOM: A FIRST AMENDMENT JURISPRUDENCE FOR THE MODERN STATE 22–23 (2012) (arguing a central distinction in First Amendment between public discourse, which the state can regulate in limited ways, and professional speech, which the state can regulate broadly to protect the interests of clients and beneficiaries).

[235] *See* Jack Balkin & Jonathan Zittrain, *A Grand Bargain to Make Tech Companies Trustworthy*, The Atlantic (Oct. 3, 2016), www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346/ (proposing that if digital businesses "agree to a set of fair information practices, including security and privacy guarantees… the federal government would preempt a wide range of state and local laws" affecting them).