PRIVACY IN THE DIGITAL AGE: IS OUR DATA SAFE?

Ezra Wolfson[†] [††]

TABLE OF CONTENTS

[†]B.A., 2017, Touro College, J.D., 2020, Benjamin N. Cardozo School of Law. The author wishes to thank first and foremost, his parents, for their unwavering support and encouragement throughout the note writing process. The author also wishes to thank Professor David Rudenstine for his advice throughout the process.

[††]At the outset, I wish to provide a vocabulary guide to several terms that will be found in this Note that refer to actions that users can perform on Facebook. 1) "Like"—a feature that enables users to easily interact with status updates, comments, photos and videos, links shared by friends, and advertisements. 2) "Share"—this feature lets people add a personalized message to links before sharing on their timeline, in groups, or to their friends via a Facebook Message. 3) "Friend"—Facebook friends aren't real friends, but are merely contacts who also have Facebook accounts who can be added by a user to increase his or her social following. 4) "Cookie"—a small piece of data a website might slide into one's smartphone or laptop to keep track of what he or she is doing online, with or without permission. 5) "Data Harvesting"—targeting a website and extracting data from that website. The data can be any type of data, including videos or simple text. *Data Mining Process: The Difference Between Data Mining & Data Harvesting* (Apr. 23, 2019), https://www.import.io/post/the-difference-between-data-mining-data-harvesting/.

I. INTRODUCTION

In 2004, Mark Zuckerberg, a 21-year-old student at Harvard University, along with several of his roommates, created the social networking platform that came to be known as Facebook.[1] Over time, Facebook has grown into one of the largest communications mediums in the world, and as of 2018, it had more than 2 billion users.[2] While the benefits of Facebook have been great, such as allowing more connectivity between users from opposite ends of the world, it also creates the potential for misuse by rouge actors who wish to infiltrate privacy of users and manipulate their identities. In recent years, it has become very easy for personal material on Facebook to be used for purposes without the user's knowledge.[3] Because of the huge trove of information stored on Facebook, it can be hard to discern accuracy from falsehoods.[4] Misinformation can spread across the platform, as

1 Nicholas Carlson*, At Last — The Full Story of How Facebook Was Founded*, BUSINESS INSIDER (Mar. 5, 2010), https://www.businessinsider.com/how-facebook-was-founded-2010-3.

2 *Number of monthly active Facebook users worldwide as of 2nd quarter 2018 (in millions)*, STATISTA, https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/ (last visited Oct. 26, 2018).

3 Jason Koebler & Joseph Cox, *The Impossible Job: Inside Facebook's Struggle to Moderate Two Billion People*, VICE (Aug. 23, 2018), https://motherboard.vice.com/en_us/article/xwk9zd/how-facebook-content-moderation-works.

4 *Id.*

was seen during the 2016 U.S. election.[5] For example, a fake newspaper called the Denver Guardian claimed that an F.B.I. agent who investigated Hillary Clinton's email disclosures had murdered his wife and shot himself.[6] The story was false, and The Denver Post published a report stating that The Denver Guardian was a hoax.[7] User information can be used for international political schemes. For example, Turkey, Venezuela, the Philippines, and more than two dozen other countries employed "opinion shapers" that spread government talking points and shut down critics within their own borders during their respective election cycles.[8] These countries used automated systems like bots and algorithms to spread their propaganda, which are new ways of disrupting democracy that are harder to track.[9] As technology improves, so do the techniques for seizing private data.[10] Digital safety has increasingly become more at risk in the years since Mr. Zuckerberg invented Facebook.[11]

This Note aims to explore the scandal that enveloped Facebook in March 2018, when it came to light that Cambridge-Analytica, a London-based data collection firm,[12] collected personal data from user

---

[5] Katie Rogers & Jonah Engel Bromwich, *The Hoaxes, Fake News and MisinFormation We Saw on Election Day*, N.Y. TIMES (Nov. 8, 2016), https://www.nytimes.com/2016/11/09/us/politics/debunk-fake-news-election-day.html.

[6] *Id.*

[7] *Id.*

[8] Jackie Snow, *Last Year, Social Media Was Used to Influence Elections in at Least 18 Countries*, MIT TECHNOLOGY REVIEW (Nov. 14), https://www.technologyreview.com/2017/11/14/3847/last-year-social-media-was-used-to-influence-elections-in-at-least-18-countries/.

[9] *Id.*

[10] Derek O'Halloran*, How Technology Will Change the Way We Work*, WORLD ECONOMIC FORUM (Aug. 13, 2015), https://www.weforum.org/agenda/2015/08/how-technology-will-change-the-way-we-work/.

[11] Evgeny Morozov*, After the Facebook Scandal It's Time to Base the Digital Economy on Public v Private Ownership of Data*, THE GUARDIAN (Mar. 31 2018), https://www.theguardian.com/technology/2018/mar/31/big-data-lie-exposed-simply-blaming-facebook-wont-fix-reclaim-private-information.

[12] David Ingram, *Factbox: Who Is Cambridge Analytica and What Did It Do?*, REUTERS (Mar. 19, 2018), https://www.reuters.com/article/us-facebook-cambridge-analytica-factbox/factbox-who-is-cambridge-analytica-and-what-did-it-do-idUSKBN1GW07F (Cambridge Analytica is an offshoot of SCL Group, a government and military contractor that says it works on everything from food security research to counter-narcotics to political campaigns. SCL was founded more than 25 years ago, according to its website. Cambridge Analytica was created in 2013, initially with a focus on U.S. elections, with $15 million in backing from billionaire Republican donor Robert Mercer and a name chosen by future Trump

accounts entailing answers that users gave in surveys administered by Facebook. This Note describes the details and timeline of breaking events. However, the Cambridge-Analytica scandal is merely the base of my discussion, the essence of this Note is to serve as a comprehensive report for user privacy on social media in general—current policy, proposed improvements, and Congressional enactments. Through choosing Facebook as a social media platform, it is easy to demonstrate risks to user privacy, particularly in light of the recent scandal. These risks include the March 2018 revelations that Cambridge Analytica, collected personal information for the Trump campaign in 2016 (which the Trump campaign then used to create political advertisements based on one's profile).[13] A further scandal that plagued Facebook occurred in September 2018, when it was reported that unknown hackers exposed the personal information of more than 50 million of its users.[14] This Note compares the 2008 Enron scandal to the recent Facebook scandals and discusses the reaction from Congress and Enron shareholders to the fallout. The Sarbanes–Oxley Act ("SOX") is used as a blueprint for the reforms that Congress should enact to protect user privacy on social media platforms. I discuss proposals by several members of the United States Senate and House of Representatives, considering whether they are adequate measures, in light of society's dependence on social media, to prevent a data breach. The Internet Bill of Rights[15] is the primary example of reforms that have been suggested by members of Congress. I compare these proposals to my proposal of "locking" data

White House adviser Steve Bannon, the New York Times reported. The company, which the New York Times reported was staffed by mostly British workers then, assisted Republican Senator Ted Cruz's presidential campaign before helping Trump's. Cambridge Analytica markets itself as providing consumer research, targeted advertising and other data-related services to both political and corporate clients. It does not list its corporate clients but on its website describes them as including a daily newspaper that wanted to know more about its subscribers, a women's clothing brand that sought research on its customers and a U.S. auto insurer interested in marketing itself).

[13] Matthew Rosenberg, et al., *How Trump Consultants Exploited the Facebook Data of Millions*, N.Y. TIMES (Mar. 17, 2018), https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.

[14] Issac, Mike & Frenkel, Sheera, *Facebook Security Breach Exposes Accounts of 50 Million Users*, N.Y. TIMES (Sept. 28, 2018), https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html.

[15] Swisher, Kara, *Introducing the Internet Bill of Rights*, N.Y. TIMES (Oct. 4, 2018), https://www.nytimes.com/2018/10/04/opinion/ro-khanna-internet-bill-of-rights.html.

found on social media to prevent any party from accessing it except for the user (including the "host," Facebook). I then discuss user remedies for those affected by the recent Facebook scandals. I explore who should be required to compensate affected users, which is dependent on Facebook's fiduciary duty to its users. I conclude with a discussion of the constitutionality of Congress penalizing Facebook by censuring or preventing users from accessing its entire platform, by comparing these circumstances to the Supreme Court's jurisprudence on freedom of the press.

II. THE CAMBRIDGE ANALYTICA SCANDAL

In March 2018, it was revealed that Facebook turned over private user data to an app called "This is Your Digital Life."[16] Aleksandr Kogan, a data scientist at Cambridge University, developed this app;[17] and in turn, Kogan provided this app to Cambridge Analytica.[18] Subsequently, Cambridge Analytica arranged an informed consent process for research, in which several hundred thousand Facebook users would agree to complete a survey for academic use only.[19] The issue, however, was that Facebook allowed this app to not only collect the personal information of the users who agreed to take the survey, but also the personal information of all the people in those users' Facebook social network.[20] Therein, Cambridge Analytica acquired data from millions of Facebook users.

In March 2018, Facebook finally revealed to the media and later to its customers that the data of up to 87 million users was improperly shared with the political consulting firm, Cambridge Analytica.[21] The data included details on users' identities, friend networks and

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

17 Carol Cadwalladr & Emma Graham-Harrison, *Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach*, THE GUARDIAN (Mar. 17, 2018), https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

18 Kurt Wagner, *Here's How Facebook Allowed Cambridge Analytica To Get Data For 50 Million Users*, VOX (Mar. 17, 2018). https://www.vox.com/2018/3/17/17134072/facebook-cambridge-analytica-trump-explained-user-data.

19 *See id.*

20 *See id.*

21 Rosenberg, *supra* note 13.

"likes."[22] This data was intended to map personality traits based on what people had liked on Facebook, and then use that information to target audiences with bespoke digital ads.[23] This process was disclosed by a whistleblower, Christopher Wylie.[24] The effect of this controversy led to a powerful firestorm of individuals calling for Facebook to look into, and revise their privacy policies and protections for users.[25] Ultimately, in the aftermath of this scandal many users discontinued their Facebook accounts, and some even went as far as to call for Facebook to shut down their app.[26]

What has not been as clear, are the corrective measures taken by Congress and the courts to fix the problem of protecting user information on social media platforms. Essentially, the question to be answered, is how such a privacy breach of personal user information can be prevented in the future, and what are the mechanisms that are needed to secure privacy while using a social media app such as Facebook.

In the aftermath of the Facebook scandal, Mark Zuckerberg testified before Congress regarding this matter.[27] The most notable exchange occurred between Zuckerberg and Senator Bill Nelson (R-FL). Senator Nelson questioned Zuckerberg regarding the Cambridge Analytica scandal, particularly Facebook's terms of service.[28] Senator Nelson and Mr. Zuckerberg spoke about Facebook's Terms of Service, its business model, and how Cambridge Analytica accessed the personal data of 87 million Facebook users.[29] During the questioning, Zuckerberg acknowledged that the first line of

22 *See id.*

23 Kieran Corcoran, *Facebook Is Overhauling Its Privacy Settings in Response to the Cambridge Analytica Scandal*, BUSINESS INSIDER (Mar. 28, 2018), https://www.businessinsider.com/facebook-overhauls-privacy-settings-after-cambridge-analytica-scandal-2018-3.

24 *See id.*

25 Alvin Chang, *The Facebook and Cambridge Analytica Scandal, Explained with a Simple Diagram*, VOX (May 2, 2018), https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram.

26 *See id.*

27 Transcript courtesy of Bloomberg Government, *Transcript of Mark Zuckerberg's Senate Hearing*, WASH. POST (Apr. 10, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/?utm_term=.2e68bf971b64 [hereinafter *Transcript of Mark Zuckerberg's Senate Hearing*].

28 *See* Kirby Wilson & Allison Graves, *Here's a Transcript of Bill Nelson's Committee Hearing Questioning of Mark Zuckerberg*, TAMPA BAY TIMES (Apr. 10, 2018), https://www.tampabay.com/florida-politics/buzz/2018/04/10/heres-a-transcript-of-bill-nelsons-committee-hearing-interview-with-mark-zuckerberg/.

29 *See id.*

Facebook's Terms of Service states that users control and own the information and content that they put on Facebook.[30] In response, Senator Nelson pointed out that when Facebook first discovered that Cambridge Analytica harvested personal user information, as early as 2015, Facebook failed to notify the affected users.[31] Zuckerberg assured Senator Nelson and the other senators on the committee that Facebook updated its policies in response to the scandal to ensure that something like this wouldn't happen again.[32] The key takeaway from the exchange between Senator Nelson and Mr. Zuckerberg was first, the exchange showed a willingness by legislators to rein in Facebook about controlling the data of its users. It demonstrated the building momentum by Congress to take decisive action in response to the data breach scandals.[33]

However, Senator Nelson pushed back and in his view stated that Facebook had not really outlined clear proposals to improve user privacy and ensure that private user privacy is protected. Senator Nelson, above all, emphasized that Facebook had to strengthen its privacy protections for its users.[34] Sen. Nelson, perhaps more than other legislators, was willing to craft a congressional response to the data breaches if Facebook did not take action.[35] Zuckerberg's response was that Facebook had "updated [its] policies," but did not actually explain how it had updated its polices.[36] However, Senator Nelson was unconvinced about Zuckerberg's vague promises of reform, saying that if "Facebook won't fix it, then the Senate will have to fix it."[37] To truly ensure that such a scandal will not happen again, there need to be clear and strong statutory and legislative reforms enacted, which will ensure that private data cannot be sold or shared with another app, and later sold to a data-collecting company. Furthermore, there need

30 *See id.*

31 *See id.*

32 *See id.*

33 Neidig, Harper & Chalfant, Morgan, *Five Takeaways From Zuckerberg's Testimony*, (Apr. 11, 2018) https://thehill.com/policy/technology/382745-five-takeaways-from-zuckerbergs-testimony.

34 Emily Tillet, *Sen. Bill Nelson Skeptical Facebook Can Address Privacy Issues*, CBS NEWS (Apr. 9, 2018), https://www.cbsnews.com/news/sen-bill-nelson-holds-press-conference-after-zuckerberg-meeting-live-updates/.

35 Wagenseil, Paul, *8 Key Takeaways From Zuckerberg's Senate Testimony*, (Apr. 10, 2018) https://www.tomsguide.com/us/zuckerberg-facebook-senate,news-26950.html.

36 Wilson & Graves, *supra* note 28.

37 *Transcript of Mark Zuckerberg's Senate Hearing*, *supra* note 27.

to be clear guidelines for how to handle such a breach, should it occur, from a moral and ethical perspective.

Further, Senator Mark Warner (D-VA), one of the most zealous critics of Facebook in the Senate, drafted a paper entitled, "The White Paper," in which he discusses the need for statutory reforms to monitor social media platforms.[38] In "The White Paper," Senator Warner expresses the urgency for fixing issues with digital platforms. With online use becoming more widespread, and the use of social media more prevalent in our society, social media platforms have developed more advanced capabilities to track and model consumer behavior—even across the multiple devices a single consumer owns.[39] This includes detailed information on viewing, window-shopping, and purchasing habits, in addition to more sensitive information.[40] Consumers are offered free services on social media in an effort to obtain their personal information, but there is a "catch"—consumers end up providing ever-more data in exchange for continued usage.[41] By providing personal profiles, users are exposing themselves to harm in undetectable ways.[42] For example, users have no reason to suspect that certain browsing behavior could likely determine the interest they pay for various purchases, and certainly gives no cause to suspect what their "friends" post.[43] Users do not know that their information is being used in these varying ways, resulting in a disconnect between reality and the user's expectations.[44]

A. The Immediate Need for Action: A Bigger Breach After Cambridge Analytica, and Facebook Does Not Seem to Care

In recent months there have been reports of hackers seeping into 50 million users' Facebook accounts.[45] Though the identities of the

---

38 Sen. Mark Warner, *Potential Policy Proposals for Regulation of Social Media and Technology Firms*, WHITE PAPER (July 23, 2018), https://www.warner.senate.gov/public/_cache/files/d/3/d32c2f17-cc76-4e11-8aa9-897eb3c90d16/65A7C5D983F899DAAE5AA21F57BAD944.social-media-regulation-proposals.pdf.

39 *See id.*

40 *See id.*

41 *See id.*

42 *See* Yousra Zaki, *The Dangers of Social Media That No One Likes to Admit*, GULF NEWS (Sept. 9, 2018, 16:34), https://gulfnews.com/opinion/thinkers/the-dangers-of-social-media-that-no-one-likes-to-admit-1.2087285.

43 *See* Warner, *supra* note 39.

44 *See id.*

45 Matt O'Brien & Mae Anderson, *Facebook Says 50M User Accounts Affected by Security Breach*, ASSOCIATED PRESS (Sept. 28, 2018),

hackers are not explicitly clear, the hackers accessed personal data through digital keys that are used by Facebook to keep users logged in.[46] The extent of the breach was such that hackers could view private messages or post on someone's account.[47] Also vulnerable to these hacks, were third-party apps that were accessed through Facebook (such as Instagram, which Facebook owns). Facebook's "tokens," mechanisms that enable one to view his or her account, allowed the hackers to use the accounts as if they were the account holders themselves. Facebook should conduct a good-faith investigation to ascertain who the hackers are. Such a good-faith investigation would include hiring data security experts to trace the movements of the hackers. The experts would search the extent of the data breach, and would see in what ways users were affected. This includes a list of the types of data that were hacked. Facebook has deep pockets, and it could spend the money necessary to perform an investigation that is thorough and well-organized. The investigation would accomplish a sense of certainty as to what the harms are, what private data was breached, and would form an idea of proper compensation for affected users.

In the aftermath of the Cambridge Analytica scandal, Senator Mark Warner expressed the urgent need for Congress to act after this latest breach, since Facebook had not responded properly to the outcries from its users over the scandals that compromised user data.[48] As is mentioned later in this Note, Facebook had taken some measures, but they simply are not enough to fully resolve the ongoing privacy concerns. It has been more than six months since Mark Zuckerberg appeared before Congress and promised lawmakers, and more importantly, the American public, that Facebook would do better and would improve.[49] But his promises are empty. Not only has Facebook not taken substantive measures, but Facebook gave advertisers contact information harvested from the address books on

https://apnews.com/65986276c04449ffb3e795ce0eef29d4/Facebook-says-50M-user-accounts-affected-by-security-breach.

46 *See id.*

47 *See id.*

48 Press Release, *Senator Warner Responds to Facebook Hack* (Sept. 28, 2018), https://www.warner.senate.gov/public/index.cfm/2018/9/sen-warner-responds-to-facebook-hack.

49 New York Times Editorial Board, *Did Facebook Learn Anything From the Cambridge Analytica Debacle?*, N.Y. TIMES (Oct. 6, 2018), https://www.nytimes.com/2018/10/06/opinion/sunday/facebook-privacy-breach-zuckerberg.html.

their users' cellphones.[50] Furthermore, Facebook gave advertisers phone numbers that users have provided solely for security reasons.[51]

1. Enron and the Guiding Light of Ethics Reform

Before I begin discussing the Enron Scandal, I chose the Enron story as my comparative baseline because it provides an effective model on how one scandal was met with a bipartisan, sweeping response by Congress. Like the Facebook scandals, the Enron scandal affected its shareholders and many of the similar duties, such as fiduciary duties (to be discussed later) were violated in both examples. The Enron Scandal surfaced in October 2001 when it became known that one of America's largest energy companies, Enron, a Houston, Texas based corporation, was involved in corporate corruption and accounting fraud.[52] The scandal led to the subsequent bankruptcy of the Enron Corporation, and the de facto dissolution of Arthur Andersen LLP, which was (at the time) one of the five largest audit and accountancy partnerships in the world.[53] In addition to being the largest bankruptcy reorganization in American history at that time, Enron was (and continues to be) cited as one of the biggest moral failures in the business community.[54] The primary cause of the scandal resulted from Enron's complex financial statements that were confusing to shareholders and analysts.[55] From a legal standpoint, numerous shareholder class action lawsuits against directors and officers of Enron were filed in the aftermath of the scandal. These lawsuits alleged violations of federal securities law, for issuing false and misleading public statements that failed to disclose the company's true financial status.[56] At the same time, a significant number of

50 Kashmir Hill, *Facebook Is Giving Advertisers Access to Your Shadow Contact Information,* GIZMODO (Sept. 26, 2018), https://gizmodo.com/facebook-is-giving-advertisers-access-to-your-shadow-co-1828476051.

51 *See id.*

52 *See* Troy Segal, *Enron Scandal: The Fall of a Wall Street Darling*, INVESTOPEDIA (Sept. 20, 2018), https://www.investopedia.com/updates/enron-scandal-summary/.

53 *See id.*

54 *See* William W. Bratton*, Does Corporate Law Protect the Interests of Shareholders and Other Stakeholders? Enron and the Dark Side of Shareholder Value*, 76 TUL. L. REV. 1276, 1280 (2002).

55 Toni Mack, *The Other Enron Story*, FORBES (Oct. 14, 2002), https://www.forbes.com/forbes/2002/1014/062.html#2f9b18f735e1.

56 *Corporate Fiduciary Liability Claims In The Post-Enron Era*, (Mar. 26, 2008) https://corporate.findlaw.com/human-resources/corporate-fiduciary-liability-claims-in-the-post-enron-era.html).

ERISA class action lawsuits were filed by employees whose retirement and stock savings plans were heavily invested in Enron's stock. The lawsuits sought to impose fiduciary liabilities on Enron, including its directors and officers.[57] In addition, its complex business model and unethical practices required that the company use accounting limitations to misrepresent earnings and modify the balance sheet to indicate favorable performance.[58] This scandal affected many shareholders, and subsequently, many shareholders filed a collective $40 billion lawsuit after the company's stock price, which achieved a high of $90.75 per share in mid-2000, plummeted to less than $1 by the end of November 2001.[59] In the aftermath of the Enron Scandal, many executives at Enron were indicted for a variety of charges, and some were later sentenced to prison.[60] Enron's auditor, Arthur Andersen, was found guilty in the United States District Court, Southern District of Texas for obstruction of justice after illegally destroying documents relevant to the Securities and Exchange Commission's ("SEC") investigation. This voided Enron's license to audit public companies, effectively closing the business.[61] By the time the ruling was overturned by the Supreme Court of the United States, Enron had lost most of its customers and had ceased all operations.[62] Ultimately, Enron employees and shareholders received limited return in lawsuits despite losing billions in pensions and stock prices.[63]

2. Legislative Response to the Enron Scandal: Sarbanes-Oxley

---

[57] Richard A. Oppel Jr., *Employees' Retirement Plan Is a Victim as Enron Tumbles*, N.Y. TIMES (Nov. 22, 2001), https://www.nytimes.com/2001/11/22/business/employees-retirement-plan-is-a-victim-as-enron-tumbles.html.

[58] *See* Paul M. Healy & Krishna G. Palepu, *The Fall of Enron*, 17 J. ECON. PERSP. 2, 9 (Spring 2003).

[59] *See Enron Shareholders Look to SEC for Support in Court*, N.Y. TIMES (May 10, 2007), https://www.nytimes.com/2007/05/10/business/worldbusiness/10iht-enron.1.5648578.html?_r=0.

[60] Alexei Barrionuevo, *Enron Chiefs Guilty of Fraud and Conspiracy*, N.Y. TIMES (May 25, 2006), https://www.nytimes.com/2006/05/25/business/25cnd-enron.html.

[61] *See* Securities and Exchange Commission v. Richard A. Causey, Jeffrey K. Skilling and Kenneth L. Lay, Civil Action No. H-04-0284 (Harmon) (S.D. Tx.) (July 8, 2004) (Second Amended Complaint)

[62] *See* Arthur Andersen LLP v. United States, 544 U.S. 696 (2005).

[63] Associated Press, *Enron's Plan Would Repay a Fraction of Dollars Owed,* N.Y. TIMES (July 12, 2003), https://www.webcitation.org/5tZ5cPyj6?url=http://www.nytimes.com/2003/07/12/business/enron-s-plan-would-repay-a-fraction-of-dollars-owed.html.

Act

Because of the scandal, new legislation and regulations were enacted to expand the accuracy of financial reporting for public companies. The Enron scandal was a major test in business ethics to which both Congress and courts responded. Congress, for example passed the Sarbanes-Oxley Act of 2002 ("SOX"). SOX is a federal law that enacted a comprehensive reform of fraudulent accounting activities.[64] SOX targets publicly held corporations, their internal financial controls, and their financial reporting audit procedures as performed by external auditing firms.[65] More specifically, SOX set new standards for public accounting firms, corporate management, and corporate boards of directors.[66] The Act received much praise from business executives, congressmen, and other important officials.[67]

A key element of SOX was the creation of the Public Company Accounting Oversight Board ("PCAOB"). PCAOB is a private-sector, nonprofit corporation created to oversee the audits of public companies and other issuers to protect the interests of investors and further public interest through the preparation of informative, accurate and independent audit reports.[68] PCAOB also oversees the audits of broker-dealers, including compliance reports filed pursuant to federal securities laws, which promote investor protection.[69] All PCAOB rules and standards must be approved by the SEC.[70]

Because of SOX, both the CEO and CFO of a corporation are now required to take ownership for their financial statements under

---

64 Will Kenton, *Sarbanes-Oxley (SOX) Act of 2002*, INVESTOPEDIA, https://www.investopedia.com/terms/s/sarbanesoxleyact.asp (last updated Feb. 4, 2020).

65 Kimberly Amadeo, *Sarbanes-Oxley Summary*: *Four Ways Sarbanes-Oxley Stops Corporate Fraud*, THE BALANCE (Oct. 27, 2019), https://www.thebalance.com/sarbanes-oxley-act-of-2002-3306254.

66 *See* Greg Farrell, *Sarbanes-Oxley Law Has Been a Pretty Clean Sweep,* USA TODAY (July 30, 2007), https://usatoday30.usatoday.com/money/companies/regulation/2007-07-29-sarbanes-oxley_N.htm.

67 Alan Greenspan, Chairman, *Commencement Address at the Wharton School, University of Pennsylvania* (May 15, 2005), https://www.federalreserve.gov/boarddocs/speeches/2005/20050515/default.htm.

68 PCAOB, https://pcaobus.org/ (last visited Sept. 28, 2018).

69 Rouse, Margaret. *PCAOB (Public Company Accounting Oversight Board)*, https://searchcompliance.techtarget.com/definition/PCAOB-Public-Company-Accounting-Oversight-Board (last visited April 29, 2020).

70 *Id.*

Section 302, which was not the case prior to SOX.[71] SOX imposed new obligations in that it requires an Internal Control Report which a company is responsible for producing to showcase its financial records.[72] For transparency, any shortfalls must be reported up the chain. SOX also requires companies to develop and implement a comprehensive data security strategy that protects and secures all financial data stored and utilized.[73] SOX requires that companies maintain and provide documentation proving they are compliant and that they are continuously monitoring and measuring SOX compliance objectives.[74] SOX has been praised for nurturing an ethical culture, as it forces top management to be transparent and employees to be responsible for their acts while protecting whistleblowers.[75]

3. Courts' Take on Ethical Obligations of Publicly Shared Companies: Transparency and Top Management Accountability

In *Skilling v. United States*, the Supreme Court held that business ethics laws must be upheld and honored.[76] "According to John J. Falvey, Jr., a white collar criminal defense attorney employed at Goodwin Procter LLP, the court's ruling was significant for narrowing the honest services fraud statute contained in 18 U.S.C. § 1346, which now means that "prosecutors must demonstrate 'palpable conduct' by someone charged with honest services fraud."[77] However, the Court's ruling did not do away with the ethical obligation that corporate executives, or other important individuals in positions of power, have to be transparent to shareholders and employees of the company, nor did it do away with the obligation to protect whistleblowers.[78] Instead, the Court simply did not address this topic. Alternatively, the Court

---

71 Ronald E. Marden, Randal K. Edwards & William D. Stout, *The CEO/CFO Certification Requirement*, CPA J. (July 3, 2003).

72 Jeff Petters, *What is SOX Compliance? Everything You Need to Know in 2019*, (updated Mar. 29, 2020) https://www.varonis.com/blog/sox-compliance/.

73 *Id*.

74 *Id*.

75 Lisa J. Banks & Jason Schwartz, *WHISTLEBLOWER LAW: A Practitioner's Guide* (2016), https://www.kmblegal.com/sites/default/files/Sample-Whistleblower-Law-Practitioners-Guide.pdf (last visited Sept. 28, 2018).

76 *See generally* Skilling v. United States, 561 U.S. 358 (2010).

77 Michael Connor, *Supreme Court Ruling Narrows Honest Services Law*, BUSINESS ETHICS (June 24, 2010), http://business-ethics.com/2010/06/24/u-s-supreme-court-provides-victory-for-enrons-skilling-narrows-honest-services-law/.

78 *Id.*

focused on the meaning and interpretation of the honest services fraud statute as it applied to the executives at Enron. In the Court's language:

> That formulation, however, leaves many questions unanswered. How direct or significant does the conflicting financial interest have to be? To what extent does the official action have to further that interest to amount to fraud? To whom should the disclosure be made and what information should it convey? These questions and others call for particular care in attempting to formulate an adequate criminal prohibition in this context.[79]

4. From the Enron Scandal to the Cambridge Analytica Scandal: Different Circumstances, Same Lessons

The fallout from the Enron scandal and the resulting ethics reforms, particularly SOX, is the blueprint for my proposed solution to the Cambridge Analytica scandal. An act like SOX in its content will make social media data-sharing apps, such as Facebook, obligated to notify users when a privacy breach occurred. Just like SOX requires publicly traded companies to be transparent with shareholders and employees and protect whistleblowers who provide key information about a breach in corporate fiduciary duty, so too, should Congress pass such an act. I would call such an act the "Social Media Transparency Act." This act would require social media companies, among other online data-sharing companies to be transparent with users if a breach were to occur and would require the protection of whistleblowers who are hired to scout out a social media company. The Act would further require social media employees to compile quarterly reports and submit them up the chain of command to the CEO and CFO. It would mandate a careful investigation of the types of data that were hacked. It would require social media companies to hire outside data security experts to assess the data that was breached. Facebook do not do this, as Zuckerberg acknowledged during the testimony.[80] When it first learned about the data collected by the third-party website and then sold to Cambridge Analytica, Facebook did not notify its users nor propose concrete steps to compensate them.[81]

Facebook, soon after the Cambridge Analytica scandal came out, pledged to inform users whose data was breached; the company

---

79 *Skilling*, 561 U.S. at 395, n. 44.

80 *See Transcript of Mark Zuckerberg's Senate Hearing*, *supra* note 27.

81 *See id.*

announced this in a statement.[82] The company further announced that users "whose information may have been improperly used by This Is Your Digital Life and Cambridge Analytica . . . will get a link to the Facebook Help Center page with a tool that will tell them if and how their data may have been misused."[83] Though Facebook pledged to undertake these measures, it did not go far enough to ensure the safety of user privacy. A congressional act that mandates these actions would provide more credibility overall.

B. Preventing a Future Data Breach—My Proposal: "Locking" Personal Information on Facebook To Prevent It From Leaving Facebook

My proposal would prevent personal and private information on Facebook from being shared by a third-party app or website. My proposal would create a mechanism whereby personal information that is stored on Facebook cannot be collected by a third-party website. One way in which this can be accomplished is by "locking" private information so that it cannot be copied or sold. Such an action could easily be spearheaded and completed by Silicon Valley tech experts who are employed by Facebook and who helped design and create the Facebook app and its features. We live in an age of technological innovation, with new inventions and features revealed to the public every day. Just like so many other technological creations have come to exist at a rapid pace,[84] this feature can be created by Facebook employees.

Besides my own proposal, Facebook has made some changes to its privacy settings shortly after the Cambridge Analytica scandal occurred. They are as follows. First, privacy controls became easier to find and use as now, privacy settings are accessible from a single place (instead of spread across nearly 20 different screens).[85] [86] Second, a

---

82 Nadeem Badshah, *Facebook to Contact 87 Million Users Affected by Data Breach*, THE GUARDIAN (Apr. 8, 2018), https://www.theguardian.com/technology/2018/apr/08/facebook-to-contact-the-87-million-users-affected-by-data-breach.

83 *Id.*

84 *See* Jochebed Menon, *Cazza to Build World's First 3D Printed Skyscraper*, CONSTRUCTION WEEK ONLINE (Mar. 12, 2017), http://www.constructionweekonline.com/article-43436-cazza-to-build-worlds-first-3d-printed-skyscraper/.

85 *It's Time to Make Our Privacy Tools Easier to Find*, FACEBOOK (Mar. 28, 2018), https://about.fb.com/news/2018/03/privacy-shortcuts/.

86 Kieran Corcoran, *Facebook Is Overhauling Its Privacy Settings in Response to the Cambridge Analytica Scandal*, BUSINESS INSIDER (Mar. 28, 2018),

new shortcut menu was added to draw several different settings together.[87] The new Privacy Shortcuts is a menu where users can more easily control their data, with clearer explanations of how privacy controls work.[88] Third, an "Access Your Information" tool was introduced to let users download the data Facebook holds on them.[89] Finally, Facebook rewrote its terms of service to better explain how it holds and uses data.[90]

However, these reforms still do not completely ensure that private data on Facebook will be fully protected from outside influence or outside sources.[91] Although Facebook, in its updated terms of services, makes clear that a user's data can no longer be freely collected by third parties,[92] nonetheless, Facebook can still share private data with "friends" of a user in connection with an ad or a promotion.[93] The language of this key update to their terms of service is as follows:

> You give us permission to use your name and profile picture and information about actions you have taken on Facebook next to or in connection with ads, offers, and other sponsored content that we display across our Products, without any compensation to you. For example, we may show your friends that you are interested in an advertised event or have liked a Page created by a brand that has paid us to display its ads on Facebook. Ads like this can be seen only by people who have your permission to see the actions you've taken on Facebook.[94]

Although Facebook assures, specifically in the last sentence of this clause, that ads that a user endorses or "likes" can be seen only be people who have the user's permission to see the actions that they have

https://www.businessinsider.com/facebook-overhauls-privacy-settings-after-cambridge-analytica-scandal-2018-3.

87 *Id.*

88 Kieran, *supra* note 87.

89 *Id.*

90 *Id.*

91 Josh Constine, *Facebook Rewrites Terms of Service, Clarifying Device Data Collection*, TECHCRUNCH (Apr. 4, 2018), https://techcrunch.com/2018/04/04/facebook-terms-of-service/.

92 *Terms of Service*, FACEBOOK (July 31, 2019), https://www.facebook.com/legal/terms/update/draft2?CMS_BRANCH_ID=1534594943262990.

93 Constine, *supra* note 92.

94 FACEBOOK, *supra* note 92.

taken on Facebook,[95] this is not enough to protect user privacy. Unless there is a "red flag" with what a person posts on Facebook, Facebook should not have any control over that content, whether by sharing it with a person who has the user's permission, or whether by using it in connection in ads, offers, or other sponsored content displayed across Facebook. How one navigates Facebook should be solely in the user's domain. The user should have complete decision-making power in how he or she regulates their activity and actions on Facebook. Once Facebook is given permission to control a user's private activity in connection with various functions, that creates a loophole for hackers and breaches by third-parties. Congress should thus pass an act that compels Facebook to create a feature that "locks" a user's posts, activity, and "likes" so that nobody, not even Facebook, is able to use it in connection with ads or the like. Such a measure will fully protect users and truly provide a safe and secure platform that is solely controlled by them, providing them with complete autonomy, without ultimate control by the host company, Facebook.

1. Other Solutions: The Internet Bill Of Rights

In a September 2018 interview, then-U.S. House of Representatives Minority Leader Nancy Pelosi, suggested that a special agency could be created to "manage tech's growing impact."[96] But she went even further, putting Rep. Ro Khanna, the Democratic representative whose California district houses many of the biggest tech companies such as Intel, Apple and Yahoo, in charge of creating a set of principles that everyone can agree upon and adhere to.[97] Rep. Khanna devised ten principles that address topics such as privacy, net neutrality, and discrimination.[98] The suggested name for this list is the "Internet Bill of Rights," which would provide "Americans with basic protections online."[99]

Mr. Khanna's list is as follows: (1) to have access to and knowledge of all collection and uses of personal data by companies;

---

95 *Id.*

96 *Nancy Pelosi's Bill of Rights*, AXIOS (Oct. 5, 2018), https://www.axios.com/nancy-pelosi-internet-bill-of-rights-2018-midterms-da342882-b710-47dc-851f-d4c2beb23d87.html.

97 *Id.*

98 Andrew Blake, *Ro Khanna, House Democrat Representing Silicon Valley, Proposes an 'Internet Bill of Rights,'* WASH. TIMES (Oct. 5, 2018), https://www.washingtontimes.com/news/2018/oct/5/rep-ro-khanna-california-democrat-proposes-interne/.

99 *Id.*

(2) to opt-in consent to the collection of personal data by any party and to the sharing of personal data with a third party; (3) where context appropriate and with a fair process, to obtain, correct or delete personal data controlled by any company and to have those requests honored by third parties; (4) to have personal data secured and to be notified in a timely manner when a security breach or unauthorized access of personal data is discovered; (5) to move all personal data from one network to the next; (6) to access and use the internet without internet service providers blocking, throttling, engaging in paid prioritization or otherwise unfairly favoring content, applications, services or devices; (7) to internet service without the collection of data that is unnecessary for providing the requested service absent opt-in consent; (8) to have access to multiple viable, affordable internet platforms, services and providers with clear and transparent pricing; (9) not to be unfairly discriminated against or exploited based on your personal data; and (10) to have an entity that collects your personal data have reasonable business practices and accountability to protect your privacy.[100] It should be noted that the fourth principle, timely notification in the event of a breach, was promised by Mr. Zuckerberg and his Facebook teams in the aftermath of the Cambridge Analytica scandal, where they pledged to be transparent with Facebook users in the event of a future breach.[101]

Given a lack of bipartisanship in Congress, such a Bill of Rights would be unlikely to garner the requisite number of votes to be passed by the House and Senate.[102] However, Mr. Khanna believes that considering numerous tech scandals, Congress is fully aware of the dangers that technology poses for affected users and is more willing to come together to regulate tech.[103] In Europe, many laws have been passed to halt tech's aggressive march towards strict control of people's privacy rights, and in California, many strong privacy laws have been passed that Congress should consider implementing.[104] Now-Speaker Pelosi promised that if Democrats were to take back the House in the 2018 midterm elections, there would be more action

100 Kara Swisher, *Introducing the Internet Bill of Rights*, N.Y. TIMES (Oct. 4, 2018), https://www.nytimes.com/2018/10/04/opinion/ro-khanna-internet-bill-of-rights.html?nytapp=true&smid=nytcore-ios-share.

101 Salinas, Sara, *Zuckerberg on Cambridge Analytica: 'We have a responsibility to protect your data, and if we can't then we don't deserve to serve you'*, CNBC (Mar. 21, 2018) https://www.cnbc.com/2018/03/21/zuckerberg-statement-on-cambridge-analytica.html.

102 *Id.*

103 *Id.*

104 *Id.*

taken to pass significant privacy laws.[105] With the House now in Democratic control, it remains to be seen how Ms. Pelosi and the Democrats will implement their proposals on privacy protection.

Another version of an "Internet Bill of Rights" has been proposed by Senator Warner. In July 2018, Senator Warner released a "white paper" containing a list of potential policy proposals for the regulation of social media.[106] "Senator Warner proposed policies that require greater disclosure by platforms—in clear, concise ways—about the types of information they collect, and the specific ways they are utilizing it."[107] The policies proposed therein are as follows: (1) Information Fiduciary—this would obligate service providers to assume special duties to respect and protect the information they obtain during their "relationship" with the consumers.[108] A fiduciary duty extends beyond a mere "tort" duty (appropriate care)—it would stipulate that service providers must pledge not to utilize or manipulate data for the benefit of the platform or third parties (rather than the user).[109] This could be established statutorily.[110] (2) Comprehensive General Data Protection Regulation (akin to the "GPDR"[111]) data protection legislation—"The U.S. could adopt rules mirroring GDPR, with key features like data portability, the right to be forgotten, 72-hour data breach notification, 1st party consent, and other major data protections."[112] "Under a regime similar to GDPR, no personal data could be processed unless it is done under a lawful basis specified by the regulation, or if the data processor has received an unambiguous and individualized consent from the data subject (1st party consent)."[113] In addition, data subjects have the right to request a portable copy of the data collected by a processor and the right to have

105 *Id.*

106 Sen. Mark Warner, *Potential Policy Proposals for Regulation of Social Media and Technology Firms*, WHITE PAPER (July 30, 2018), https://www.warner.senate.gov/public/_cache/files/d/3/d32c2f17-cc76-4e11-8aa9-897eb3c90d16/65A7C5D983F899DAAE5AA21F57BAD944.social-media-regulation-proposals.pdf.

107 *Id.*

108 *Id.*

109 *Id.*

110 *Id.*

111 See *infra* notes 108-20 and accompanying text for a brief explanation and overview of the GDPR.

112 WHITE PAPER, s*upra* note 107; *see* Matthew Ingram, *Leaked White Paper Proposes Congressional Regulation of Social Media*, Colum. Journalism Rev. (Oct. 9, 2018).

113 *Id*.

their data erased.[114] Businesses must report any data breaches within 72 hours if they have an adverse effect on user privacy.[115] One major tenant of the GDPR (that the US could or could not adopt) is the potential of high penalties for non-compliance in which a company or organization can be fined (in the EU, penalties are up to 4% of its annual global turnover or €20 million - whichever is higher).[116] (3) First Party Consent for Data Collection—The U.S. could adopt one specific element of GDPR: requiring first party consent for any data collection and use.[117] This would prevent third-parties from collecting or processing a user's data without their explicit and informed consent.[118]

Senator Warner's proposals would require bipartisan support and it is unlikely that Republicans would be in agreement with the proposed measures.[119] Simply, a Republican-controlled Congress is not likely to support these initiatives. It is more likely that government agencies will adopt some elements of his proposals independently through the rule-making process or some of the ideas will be implemented by individual states.[120] However, Senator Warner expressed confidence that a broad bipartisan majority in Congress will back the regulation of social media (including his proposals) though such legislation might take time to come together.[121] Lawmakers of both parties have criticized social media companies' efforts to rein in hacking, data breaches, and misinformation.[122]

---

114 *Id*.

115 *Id*.

116 *Id*. *See* Ariel Shapiro, *Democratic Sen. Warner Has a New Policy Paper With Proposals to Regulate Big Tech Companies*, CNBC (July 30, 2018), https://www.cnbc.com/2018/07/30/sen-warner-proposes-20-ways-to-regulate-big-tech-and-radically-change.html.

117 *Id.*

118 WHITE PAPER, *supra* note 107.

119 Adi Robertson, *Sen. Mark Warner Floats Major Tech Company Regulations That Don't Include Breakups*, THE VERGE (July 30, 2018), https://www.theverge.com/2018/7/30/17629854/mark-warner-tech-company-legislation-white-paper-privacy-misinformation-competition.

120 *Id.*

121 Steven T. Dennis & Ben Brody, *Congress Is Likely to Support New Regulations on Social Media, Senator Says*, BLOOMBERG (Sept. 13, 2018), https://www.bloomberg.com/news/articles/2018-09-13/new-social-media-rules-can-get-majority-in-congress-warner-says.

122 *Id.*

2. Incentivizing Social Media Companies to Ramp Up Protection

In light of the complexity of social media services and the sheer quantity of service providers in the digital age, Congress may find it difficult to draw lines between required tasks of social media companies and those that should not be required.[123] Three ways to foster an easier path to reform social media companies is through tax breaks, safe harbors, and legal immunities.[124] Organizations should be offered incentives to accept fiduciary obligations rather than simply imposing them directly through government regulation.[125] Therefore, as Jonathan Zittrain[126] has suggested, it might be appropriate to offer online service providers an incentive to designate themselves as information fiduciaries in return for certain legal and financial benefits that come with the designation.[127] Professor Jack Balkin[128] argues that, even though social media companies are privately owned, governments could create framework statutes that would require platform owners to respect the free speech and privacy rights of end users in return for special legal status and benefits.[129] We might be able to adapt this idea to today's online service providers to create new classes of digital information fiduciaries.[130]

123 Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1229 (2016).

124 *Id.*

125 *Id.*

126 Jonathan Zittrain is the George Bemis Professor of International Law at Harvard Law School. He is also a professor at the Harvard Kennedy School of Government, a professor of computer science at the Harvard School of Engineering and Applied Sciences, director of the Harvard Law School Library, and co-founder and director of Harvard's Berkman Klein Center for Internet & Society. *See* Jonathan Zittrain, https://hls.harvard.edu/faculty/directory/10992/Zittrain (last visited April 7, 2020).

127 *Id.* (citing Jonathan Zittrain, *Facebook Could Decide an Election*, NEW REPUBLIC (June 1, 2014), http://www.newrepublic.com/article/117878/information-fiduciary-solution-facebook-digital-gerrymandering).

128 Jack M. Balkin is Knight Professor of Constitutional Law and the First Amendment at Yale Law School. He is the founder and director of Yale's Information Society Project, an interdisciplinary center that studies law and new information technologies. He also directs the Abrams Institute for Freedom of Expression, and the Knight Law and Media Program at Yale. *See Jack M. Balkin*, https://law.yale.edu/jack-m-balkin (last visited Oct. 23, 2018) .

129 Balkin, *supra* note 124, at 1230.

130 *Id*.

C. Europe's Sweeping New Privacy Rules: GDPR

In April 2016, the European Union ("EU") introduced sweeping new privacy rules aimed at protecting consumer data stored on social media platforms and other tech websites.[131] This not only applies to companies in the EU, but also applies to companies outside the EU who provide services to users in the EU.[132] The GDPR was enacted in April 2016. The predecessor to the GDPR was the Data Protection Directive (the "DPD").[133] The DPD was adopted in 1995, at a time when the internet was in its infancy.[134] The Data Protection Directive is built on seven principles that were gathered from prior policy enactments; these proposals include:

1. Notice – individuals should be notified when their personal data is collected
2. Purpose – use of personal data should be limited to the express purpose for which it was collected
3. Consent – individual consent should be required before personal data is shared with other parties
4. Security – collected data should be secured against abuse or compromise
5. Disclosure – data collectors should inform individuals when their personal data is being collected
6. Access – individuals should have the ability to access their personal data and correct any inaccuracies
7. Accountability – individuals should have a means to hold data collectors accountable to the previous six principles.[135]

---

131 PBS News Hour, *EU to Install Sweeping Changes to Online Privacy Rules* (May 20, 2018), https://www.pbs.org/newshour/show/eu-to-install-sweeping-changes-to-online-privacy-rules.

132 Aarti Shahani, *Europe's New Online Privacy Rules Could Protect U.S. Users Too*, NPR (Apr. 16, 2018), https://www.npr.org/sections/alltechconsidered/2018/04/16/602851375/europe-s-sweeping-privacy-laws-prompt-new-norms-in-u-s.

133 Nate Lord, *What is the Data Protection Directive? The Predecessor to the GDPR*, DIGITAL GUARDIAN (Sept. 12, 2018), https://digitalguardian.com/blog/what-data-protection-directive-predecessor-gdpr.

134 *The History of the General Data Protection Regulation*, EUROPEAN DATA PROTECTION SUPERVISOR, https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en (last visited Oct. 29, 2019).

135 *Id.*

The GDPR supersedes the DPD as it fully phased out the DPD and became national law for all EU Member States on May 25, 2018.[136] The GDPR builds on the key components of the DPD with more specific data protection requirements, a global reach, and harsher enforcement as well as non-compliance penalties.[137] As a result, citizens will have more control over their personal data and more recourse if personal data is misused, while data controllers and processers will be required to protect sensitive personal data by design.[138] Finally, the GDPR offers a much simpler regulatory environment for businesses that collect or process EU citizens' and residents' personal data.[139]

The GDPR provides users with more control over their data than did the DPD, as the GDPR adapted to the advanced technology that big-tech firms now use. The GDPR considers this fact by implementing more protection for consumers than did the DPD.[140] Users will now be able to access their personal data and find out where and for what purpose it is being used.[141] Additionally, users will have the right to be "forgotten," which means that a user can request that whoever is controlling their data to erase it and potentially stop third parties processing it.[142] Another provision allows people to take their data and transfer it to a different service provider.[143]

The central tenet of EU's new privacy protections provides that companies that collect, or mine, personal data must first request consent from users.[144] The new rules will also make it harder for ad-

136 Shahani, *supra* note 133.

137 *General Data Protection Regulation GDPR*, GDPR, https://gdpr-info.eu/ (last visited Oct. 26, 2018).

138 Sagara Gunathunga, *All You Need to Know About GDPR Controllers and Processors,* MEDIUM (Sept. 12, 2017), https://medium.com/@sagarag/all-you-need-to-know-about-gdpr-controllers-and-processors-248200ef4126.

139 Angela Stringfellow, *The Ultimate Guide to GDPR Compliance: What Your Company Needs to Know to Ensure Compliance and Minimize Risk (with Checklist*), NG DATA (Jan. 22, 2018), https://www.ngdata.com/gdpr-compliance-guide/.

140 Elizabeth Schultze*, GDPR: How Europe's New Privacy Law Is Creating Big Business Opportunities*, CNBC (May 25, 2018), https://www.cnbc.com/2018/05/25/gdpr-europe-new-privacy-law-is-creating-big-business-opportunities.html.

141 *Id.*

142 *Id.*

143 *Id.*

144 Nate Lord, *What is General Data Protection Regulation? Understanding and Complying with GDPR Data Protection Requirements*, DATA INSIDER (Sept. 19, 2018), https://digitalguardian.com/blog/what-gdpr-general-data-protection-regulation-understanding-and-complying-gdpr-data-protection.

targeting companies to collect and sell this information.[145] Additionally, users can ask companies what personal information is stored, and then request that it be deleted.[146] With this said, there are severe penalties for companies who break these rules, such as a heavy fine of four percent of a company's profits.[147]

1. The United States and the GDPR

The EU's privacy protections will extend to social media users in the United States as well. As an example, Facebook announced that the EU's privacy rights will extend to its users around the world.[148] Also, American companies operating in Europe (or who serve EU citizens) must comply.[149]

It is not certain if the United States Congress will adopt a similar measure like the GDPR to formally protect users in the United States.[150] There are several reasons why a law like the GDPR would be difficult for Congress to enact. Firstly, there isn't an agency to carry out such a law.[151] Unlike EU member states, the U.S. does not have its own data privacy authorities to enforce the GDPR.[152] The closest equivalent is the Federal Trade Commission (the "FTC"), which is the main agency that enforces U.S. privacy policy.[153] But its powers are limited compared to its European counterparts.[154] Although states have their own laws and regulations concerning data privacy, there is no mechanism in the federal government to bring it under one roof.[155]

---

145 *Id.*

146 *Id.*

147 Nate Lord, *GDPR Compliance: The Impact on Infosec in 2018 and Beyond*, DIGITAL GUARDIAN (Aug. 9, 2017), https://digitalguardian.com/blog/gdpr-compliance-infosec-impact-2018.

148 Schultze, *supra* note 141.

149 Yaki Faitelson, *Yes, The GDPR Will Affect Your U.S.-Based Business*, (Dec. 4, 2017) FORBES, https://www.forbes.com/sites/forbestechcouncil/2017/12/04/yes-the-gdpr-will-affect-your-u-s-based-business/#d4bcc776ff26.

150 Derek Hawkins, *The Cybersecurity 202: Why a Privacy Law Like GDPR Would Be a Tough Sell in the U.S.*, WASH. POST (May 25, 2018), https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/05/25/the-cybersecurity-202-why-a-privacy-law-like-gdpr-would-be-a-tough-sell-in-the-u-s/5b07038b1b326b492dd07e83/?noredirect=on&utm_term=.ccd4529e5299.

151 *Id.*

152 *Id.*

153 *Id.*

154 *Id.*

155 Hawkins, *supra* note 151.

The second reason for the unlikelihood of such a bill gaining traction in Congress is due to a lack of support.[156] Given the gridlock in the current Congress, something as complex as GDPR will not likely get approved.[157] Smaller bills have been proposed though, in the aftermath of the Cambridge Analytica scandal. One of those proposed bills by Senator Warner, mentioned earlier in this Note, would expand the FTC's authority and impose new restrictions on data collection, and another bill that would give people greater control over what companies can do with their information.[158] But these are only proposals, and a bill as sweeping as the GDPR would be even more difficult to pass.

Besides the gridlock in Congress, any GDPR-like proposal would face resistance from the powerful tech lobbies, as well as lawmakers who oppose excessive taxes.[159] With the GDPR primarily focused on protecting European users from large U.S.-headquartered service providers like Google, Apple, Facebook, and Amazon, some policymakers see the GDPR as a mechanism for the E.U. to enforce privacy law, and a U.S. bill should similarly personify the spirit of the GDPR in enforcing U.S. privacy law.[160] Given President Trump's electoral mandate to regulate and tax less, Congress is not eager to penalize or tax U.S. corporations (so long as the Republican party maintains control of at least one house of Congress).[161]

As far as citizen support for Congress to enact sweeping GDPR-like legislation, some argue that there is enough U.S. support (from citizens) for a sweeping overhaul like GDPR.[162] Some point to Americans enthusiasm in supporting data privacy regulation.[163] The Cambridge Analytica scandal increased awareness of this issue.[164] There are thus valid arguments for the position that Congress should

156 *Id.*; *See also* Elias Chachak, *Will the U.S. Adopt Similar GDPR Privacy Concerns?*, CYBERDB (Oct. 23, 2018), https://www.cyberdb.co/will-u-s-adopt-similar-gdpr-privacy-concerns/.

157 Chachak, *supra* note 157.

158 *Id.*

159 *Id.*

160 *Id.*

161 Hawkins, *supra* note 151.

162 *See* Hawkins, *supra* note 151.

163 Hawkins, *supra* note 151.

164 *Id*. *See* Nellie Bowles, *After Cambridge Analytica, Privacy Experts Get to Say 'I Told You So,'* N.Y. TIMES (Apr. 12, 2018), https://www.nytimes.com/2018/04/12/technology/privacy-researchers-facebook.html.

pass a bill that echoes the GDPR, as there is strong evidence that public interest for privacy protections in tech is very high.

Although no such privacy bill has been enacted by Congress thus far, on January 1, 2020, a landmark consumer privacy law went into effect in California.[165] The California Consumer Privacy Act, or CCPA, has been likened to the GDPR and is similar to the sweeping EU law, at least in spirit, if not in practice.[166] The law allows any California consumer to demand to see all the information that is stored by a company pertaining to them.[167] The California law also allows consumers to bring an action against a company if the law's privacy guidelines are violated, even if there is no breach of data.[168]

The CCPA is less sweeping than the GDPR in several key respects. The GDPR's laws apply to all forms of businesses—any business entity that handles personal data from EU consumers must comply with the GDPR. However, the CCPA only affects for-profit entities whose business meets at least one of the following characteristics: (1) Has an annual gross revenue of at least $25 million (2) Collects, buys, sells or shares the data of at least 50,000 consumers, devices, or households in California.[169] Another important difference is that the CCPA's protections are limited to individual data subjects that legally reside in California, whereas the GDPR protects all "data subjects" (those individuals to whom the data belongs) regardless of their residence or citizenship status.[170]

It is interesting to note that both the GDPR and the CCPA have similar definitions for the term "personal data"—any information that can directly, or indirectly, represent an identifiable person.[171] But they

---

165 Devin Coldewey, *The California Consumer Privacy Act Officially Takes Effect Today*, TECH CRUNCH (Jan. 1, 2020), https://techcrunch.com/2020/01/01/the-california-consumer-privacy-act-officially-takes-effect-today/.

166 Navdeep K. Singh, *What You Need to Know About The CCPA and The European Union's GDPR*, (Feb. 26, 2020), https://www.americanbar.org/groups/litigation/committees/minority-trial-lawyer/practice/2020/what-you-need-to-know-about-the-ccpa-and-the-european-unions-gdpr/.

167 Maria Korolov, *California Consumer Privacy Act (CCPA): What you need to know to be compliant*, CSO (Oct. 4, 2019), https://www.csoonline.com/article/3292578/california-consumer-privacy-act-what-you-need-to-know-to-be-compliant.html.

168 *Id.*

169 *Id*.

170 Geoffroy De Coomon, *GDPR and CCPA Compliance: The 5 Differences You Should Know*, PROXYCLICK BLOG (Oct. 7, 2019) https://www.proxyclick.com/blog/gdpr-and-ccpa-compliance-5-differences.

171 *Id*.

vary as to various categories of data collection. Under the CCPA, "collecting" data, "selling data," and "processing" data, are all defined differently.[172] Under the GDPR, there is only one act of "processing" data, which includes everything from the initial act of collecting user data, to storing that information, making it available for others to access, and to its eventual removal.[173]

Other states have taken similar steps to enact laws similar to the CCPA. Nevada and Maine have already passed privacy laws.[174] Six other states, including New York, have introduced draft bills that would impose broad obligations on businesses to provide consumers with transparency and control of personal data.[175] More than twenty states in total are considering privacy legislation.[176] After the CCPA passed, tech companies voiced concerns that they could potentially have to contend with fifty different privacy laws.[177] Companies such as Facebook and Google argue that it would be more harmonious to have one federal law that covers the entire nation.[178] As more states follow California's lead with new privacy laws, there will likely be increased pressure on the federal government to enact a uniform law.[179]

III. USER REMEDIES: CLASSIFYING DIGITAL DATA AS "PROPERTY" THAT MUST BE COMPENSATED WHEN SUCH DATA IS COLLECTED

Many scholars believe that private data on Facebook is considered "property," and that we own our data, such that we should be compensated when someone, such as Cambridge Analytica uses it.[180] They argue that it should be like "buying" a house, where the

172 *Id*.

173 *Id*.

174 Andrea Little Limbago, *DIY data protection: As Congress Stalls, States Take Charge*, GCN (Mar. 23, 2020), https://gcn.com/articles/2020/03/23/states-lead-data-privacy-protections.aspx.

175 Hautala, Laura. *California's new privacy rights could come to your state, too* (Jan. 3, 2020) https://www.cnet.com/news/californias-new-ccpa-privacy-rights-could-come-to-your-state-too/.

176 *Id*.

177 *Id*.

178 *Id*.

179 *Id*.

180 Brittany Kaiser, *Facebook Should Pay Its 2bn Users for Their Personal Data*, FINANCIAL TIMES (Apr. 9, 2018), https://www.ft.com/content/7a99cb46-3b0f-11e8-bcc8-cebcb81f1f90.

seller is compensated for the sale.[181] Because Facebook has control over all the data contained on its app, Facebook should update its terms of services to outline compensation policies for its users.[182] It should then return benefits to the two-billion users who are responsible for Zuckerberg's success.[183] Indeed, Zuckerberg told lawmakers that "users own their online data" in his hearing.[184] He further implied that users' data is their personal property.[185]

Some scholars have hesitated calling personal, digital data "property" in the ownership and compensation context.[186] (On the other hand, some courts have also determined that data should be considered property).[187] There is an overarching concern that classifying data as property will impede the privacy protection that it is designed to create.[188] It may encourage private transactions between data holders that should be avoided.[189] Another concern is that it "will lead people to sign away" a large amount of their data.[190] In this sense, creating a property right on digital data will defeat the purpose of defending privacy, since more data will be exposed by people willing to "sell" and "do business" with their data. A related concern with propertizing data is that it would make privacy dependent on economic status.[191] The argument is that the wealthier are better suited to hold onto their data, as they are not in dire need of selling it for extra money, whereas those less well-off will be forced into selling their data to earn badly needed money.[192] Another, more theoretical objection, regarding classifying data as property, is that it will not comport with a key component of property—free alienability. Those, who take this view, hold of the premise that "property connotes free alienability."[193]

---

181 *Id.*

182 *Tell Facebook: Our Data is Our Property #OwnYourData*, CHANGE.ORG, https://www.change.org/p/tell-facebook-our-data-is-our-property-ownyourdata (last visited Sept. 28, 2018).

183 *Id.*

184 *Transcript of Mark Zuckerberg's Senate Hearing*, *supra* note 27.

185 *Id.*

186 *See* Wanling Su, *What is Just Compensation*? 105 VA. L. REV. 8, 12 (2019).

187 Carpenter v. United States, 585 U.S. ___ (2018).

188 Michael C. Pollack, *Taking Data*, 86 U. CHI. L. REV. 77, 108 (2019) (citing Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1303 (2000)).

189 *Id.*

190 *Id.*

191 *Id.* at 109.

192 *Id.*

193 *Id.* at 110 (citing Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2056, 2091 (2004)).

Because of concerns with propertized data being freely sold on the market, which threatens privacy, there will be limitations imposed on one's data ownership, thus weakening the alienability of propertized data.[194] This will lead to a type of property that is not truly property.[195]

However, the premise that something can only be classified as property, if that thing is freely and fully alienable, is refutable. Various examples of restricting alienation both on the real property and intellectual property sides prove that even if property is not fully alienable, it is still called property. On the real property side, there are conservation easements and historic preservation laws that function as restraints on property.[196] On the intellectual property side, statues like the Video Privacy Protection Act of 1988, the Driver Privacy Protection Act of 1994, and the Gramm-Leach-Bliley Act of 1999, either prohibit entities altogether from transferring the information they possess in their files or impose conditions on the circumstances under which transfers can occur and on those to whom such information can be transferred.[197] In these examples of free alienation restrictions, there is no question that the property burdened by those restrictions was called property. This demonstrates that restrictions on free alienation can easily coexist with property status.[198] Thus, it is possible to propertize data and still establish privacy-protecting limitations on the transfer of data, since the two can coexist. As such, propertizing data should be fully embraced, and not looked down upon.[199]

Courts have considered government intrusions on personal property as the taking of a property right that requires compensation.[200] As the Supreme Court has explained, such "property concepts" are instructive in "determining the presence or absence of the privacy interests protected by the Fourth Amendment."[201] The *Jones* opinion emphasizes that the text of the Fourth Amendment reflects the Amendment's "close connection to property,"[202] as the text of the Amendment refers to various types of property—"houses,

194 Pollack, *supra* note 189, at 110.

195 *Id.*

196 *Id.* at 111 (citing RESTATEMENT (THIRD) OF PROPERTY: Servitudes § 3.4, cmt. f at 445 (2000)).

197 *Id.* at 112 (citing Schwartz, 117 HARV. L. REV. at 2099–2101).

198 *Id.* at 113.

199 *Id.* at 113–14.

200 *Id.* at 81.

201 *Id.* at 113 (citing *Byrd*, 138 S. Ct. at 1526).

202 *Id.* at 113 (citing *United States v. Jones*, 565 U.S. 400, 405 (2012)).

papers, and affects."[203] The British common law that existed during the period in which the Fourth Amendment was adopted, also expressed the concept of a search as one in which an unconsented entry onto property occurred.[204] Of course, while the Court held in *Katz v. United States* that a search for Fourth Amendment purposes occurs whenever the government violates a person's "reasonable expectation of privacy,"[205] the Court has also consistently cautioned that the *Katz* test "supplements, rather than displaces" the traditional property-based tests.[206] "Accordingly, principles of property law remain quite relevant in assessing and governing the kinds of investigatory activity in which the government may engage."[207]

A similar framework should be adopted to establish compensation for personal users when a *private corporation* steals or accesses their digital property. Although affected uses don not have a Taking Clause claim—since Facebook and other social media companies are private corporations and not government entities—the users are entitled to compensation solely based on a property law basis.

A. Tort Remedies For Affected Users

In the U.K., Facebook users who were the target of a cyber-attack could possibly have received £12,500 if they could prove distress resulting from the data breach.[208] Professor Maureen Mapp of Birmingham University Law School estimated this amount based on the amount that was awarded to six Brits who were phone-hacked by the *Mirror* newspaper in 2015.[209] Any citizen who wished to collect the money, had to sue under the U.K.'s Data Protection Act and prove that the breach had caused them distress.[210] The amount of compensation for each affected user would depend on the amount of

203 *Id.* at 113 (citing *Jone*s, 565 U.S. at 404).

204 *Id.* at 113 (citing *Jones*, 565 U.S. at 404–05).

205 Pollack, *supra* note 189, at 113 (citing *Katz v. United States*, 389 U.S. 347, 360 (1967)).

206 *Id.* at 113 (citing *Byrd*, 138 S. Ct. at 1526).

207 *Id.* at 113 (citing *Byrd*, 138 S. Ct. at 1526); *cf. Carpenter v. United States*, 138 S. Ct. 2206, 2209 (2018).

208 Nicholas Bieber, *Brits Could Get £12,500 EACH from Facebook Over Massive Data Breach*, DAILY STAR (Mar. 29, 2018), https://www.dailystar.co.uk/news/latest-news/692253/Facebook-lawsuit-Cambridge-Analytica-data-breach-login-compensation.

209 *Id.*

210 *Id.*

distress suffered.[211] There is no standard formula to calculate this non-economic damage. It would vary on a case by case basis.[212] This damage is a subjective damage and differs depending on a plaintiff's personal or subjective experience.[213] To recover non-economic damages, the plaintiff must show by a preponderance of the evidence that they suffered those injuries.[214] However, David Barda, a data protection lawyer for Slater and Gordon (a large consumer law firm based in Australia) has stated that a more realistic amount of £500 could be awarded for those who met the distress threshold.[215] If, indeed, each user affected could demonstrate that the data breach caused him or her distress, this could result in an astronomical loss for Facebook, which would severely jeopardize the company.[216] This would be calculated by multiplying the damage award for each affected user (12,500) by the number of affected users (50 million).[217]

In the United States, there has been some discussion among the courts about civil damages for affected users in data breach litigation. The United States Court of Appeals for the 9th Circuit, in *In re Zappos*[218] stated that the circuit courts now agree that plaintiffs need only allege an increased risk of identity theft to establish their constitutional right to sue the businesses that left their personal information vulnerable to hackers.[219] The *Zappos* court has asked the United States Supreme Court to resolve the issue of standing for data breach victims whose information was not misused.[220] But regardless, according to a consensus of federal circuit courts, plaintiffs whose personal sensitive data was breached have constitutional standing to litigate their claims.[221]

---

211 *Id.*

212 *Damages & Compensation for Mental Anguish in a Personal Injury Case*, https://www.alllaw.com/articles/nolo/personal-injury/damages-compensation-mental-aguish.html (last visited Apr. 7, 2020).

213 *Id*.

214 *Id.*

215 *Id.*

216 *Id.*

217 *Id.*

218 In re Zappos.com, Inc., 888 F.3d 1020 (9th Cir. 2018), cert. denied sub nom. Zappos.com, Inc. v. Stevens, 139 S. Ct. 1373, 203 L. Ed. 2d 609 (2019).

219 Alison Frankel, *D.C. Judge: No Actual Damages, No Claims For Data Breach Victims*, REUTERS (Feb. 4, 2019), https://www.reuters.com/article/legal-us-otc-data-breach/dc-judge-no-actual-damages-no-claims-for-data-breach-victims-idUSKCN1PT23W.

220 *Id*.

221 *Id*.

As to damage claims, Judge Cooper of the District Court for the District of Columbia wrote last year in the *Attias*[222] decision as follows: "The court acknowledges the difficulty of applying traditional tort and contract principles in the contemporary context of data security . . . . It also recognizes that courts across the country have divided on a number of important legal issues that frequently arise in data breach litigation."[223] Judge Cooper specifically observed that allegations sufficient to establish constitutional standing does not necessarily amount to an adequate claim for damages. He pointed to the 9th Circuit decision in *Krottner v. Starbucks*,[224] one of the first rulings to address standing for victims of data theft. In that case, the court deemed that plaintiffs have standing as to an increased risk of identify theft, but declined to award civil damages to the plaintiffs.[225]

Thus far, the United States Supreme Court has denied certiorari to decide the issues of constitutional standing in data breach litigation and whether users should be awarded damages in a successful action.[226]

Emotional distress for which affected users may receive compensation includes pain and suffering. In Australia, lawmakers concluded that data firms which experienced a data breach would indeed be required to pay damages to users for pain and suffering from the breach.[227] Such legislation replaced outdated legislation and includes an emphasis on data privacy.[228] Included in this legislation are guidelines for civil penalties for consumers who experience "serious harm," which includes "physical, psychological, emotional, economic and financial harm, as well as harm to reputation."[229] In February 2018, this became law in Australia with the passage of the Privacy Amendment Act.[230] The Act requires firms that experience a

222 Attias v. CareFirst, Inc., 365 F.Supp.3d 1 (D.D.C. 2019).

223 *Id.* at 10.

224 Krottner v. Starbucks Corp., 628 F.3d 1139 (9th Cir. 2010).

225 *Id*. at 1142.

226 Frankel, *supra,* note 219.

227 Paul Roberts, *Down Under, Lawmakers Ponder Pain and Suffering from Breaches*, DIGITAL GUARDIAN: DATA INSIDER (Oct. 11, 2016), https://digitalguardian.com/blog/down-under-lawmakers-ponder-pain-and-suffering-breaches.

228 *Id.*

229 *Id.*

230 Xiaoyan Zhang, *Australia's New Breach Notification Law In Effect*, REEDSMITH (Feb. 28, 2018), https://www.reedsmith.com/en/perspectives/2018/02/australias-new-breach-notification-law-in-effect.

breach to notify their users when "serious harm" is likely to result in any of the affected users.[231] In the event of a data breach, pain and suffering and all the factors listed above are part of civil penalties slapped on firms where the breach takes place.[232]

In the United States, the notion of a civil penalty for pain and suffering (including distress) in the event of a data breach is especially important considering recent data privacy scandals such as the Facebook-Cambridge Analytica report. Forty-six states, including the District of Columbia, have passed separate data notification laws.[233] U.S. courts have been conflicted regarding the definition of "harm," and whether affected consumers have suffered a harm that gives them standing to sue.[234] Meanwhile, in the U.S., the absence of a federal standard for what constitutes a "breach," whether breaches constitute "harm," and what "harm" means is likely to leave consumers with little in the way of concrete legal and civil remedies from breached firms.[235] To fix this problem, there should be a clear definition of tort remedies for pain and suffering for affected users in the advent of a data breach. Congress can accomplish this and states themselves should have a clear definition and standard for this.

1. Obligating Facebook to Compensate User Property: Information Fiduciary

Now that we have established that digital data is considered property, and is subject to compensation, we must determine *who* is required to compensate the affected users. The answer is that Facebook bears that obligation. As a publicly-held corporation, Facebook should bear the responsibility of compensating the affected users even if the digital property was collected or hacked by a third-party since Facebook violated its *information fiduciary duty* in the process of the hacking and data-collecting.[236]

The concept of Facebook assuming a fiduciary role in relation to its users is based on the idea formulated by Professor Jack Balkin.[237] Professor Balkin coined the term "information fiduciary" to explain

231 *Id.*

232 *See id.*

233 Roberts, *supra* note 228.

234 *Id*.

235 *Id*.

236 *Facebook Data Policy*, FACEBOOK, https://www.facebook.com/policy.php (last updated Apr. 19, 2018).

237 *See supra* note 129 (discussing a brief biography of Professor Balkin).

the duty that Facebook, and other social media companies, must protect user data stored on their platforms.[238] A "fiduciary" is one who is entrusted to protect the interests of another person, thing, or entity.[239] The client puts their trust and confidence in the fiduciary, and the fiduciary has a duty to protect that interest.[240] Fiduciaries essentially have two duties, the duty of care and the duty of loyalty.[241] Fiduciary duties are duties of trust, as the Latin word for trust is "fiducia."[242]

In the digital age that we are living in, Professor Balkin argues that social media companies have a fiduciary duty akin to professional relationships.[243] That does not mean that this relationship is identical to traditional, professional relationships in all respects, but, to an extent, the concept of "information fiduciary" will obligate data companies, such as Facebook in trust and loyalty.[244] Professor Balkin quotes Neil Richards[245] as stating that "in the Age of Information should we expand our definition of information fiduciaries to include bookstores, search engines, ISPs, email providers, cloud storage services, providers of physical and streamed video, and websites and social networks when they deal in our intellectual data."[246] Professor Balkin explains the reasoning behind the "information fiduciary" relationship, which depends on the foundation of a fiduciary duty in the first place. The dependence that users have on companies such as Facebook, in addition to the vulnerability of users when using these companies, are the main reasons.[247] Because social media companies possess valuable information that can be used to the detriment of users, social media companies accept upon themselves a special fiduciary

238 Balkin, *supra* note 124.

239 *Fiduciary*, GOOGLE DICTIONARY.

240 *See* Nathan Heller, *We May Own Our Data, But Facebook Has a Duty to Protect It*, THE NEW YORKER (Apr. 12, 2018), https://www.newyorker.com/tech/annals-of-technology/we-may-own-our-data-but-facebook-has-a-duty-to-protect-it.

241 *See id.*

242 *Id.*

243 *See* Balkin, *supra* note 124, at 1221.

244 *Id.*

245 Neil Richards, the Koch Distinguished Professor in Law at the Washington University in St. Louis School of Law, is one of the world's leading experts on privacy law.

246 *Id.* (citing NEIL RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE 168 (2015)).

247 *See id*. at 1222.

duty that goes beyond their corporate fiduciary duty.[248] The social media companies present themselves to the public as responsible and upstanding about their implied duty to the public, and to never betray their users.[249] This theory is an *implied* fiduciary duty arising from the status of the users vis-à-vis the provider, and from the implied trust of users in the providers which are *induced* by the providers.[250]

Professor Balkin sets forth three conditions that apply to information fiduciaries:

> (1) when these people or entities hold themselves out to the public as privacy-respecting organizations in order to gain the trust of those who use them; (2) when these people or entities give individuals reason to believe that they will not disclose or misuse their personal information; and (3) when the affected individuals reasonably believe that these people or entities will not disclose or misuse their personal information based on existing social norms of reasonable behavior, existing patterns of practice, or other objective factors that reasonably justify their trust.[251]

These three conditions are present in the relationship between Facebook and its users: inducement of trust, appearance of respect for data of privacy, reason to believe that Facebook will not disclose or misuse their personal information, and expectancy of users that Facebook will not disclose their private data based on existing norms of reasonable behavior.

Professor Balkin acknowledges that there are fundamental differences between online service providers and traditional fiduciary duties. There are significant inconsistences in the information that service providers contain and user knowledge.[252] Also, users can find it difficult to verify online companies' representations about data collection, security, and use.[253] Third, data users cannot easily understand what online companies do with their data.[254] Finally, users cannot monitor the companies' information-collecting practices.[255]

---

248 *Id*. (citing, e.g., *Community Standards*, FACEBOOK, https://www.facebook.com/communitystandards (last visited Feb. 29, 2016) ("We want people to feel safe when using Facebook.")).

249 Balkin, *supra* note 124, at 1222.

250 *See* Heller, *supra* note 241; *see* Balkin, *supra* note 124, at 1222.

251 Balkin, *supra* note 124, at 1223–24.

252 *See id.* at 1227.

253 *Id.*

254 *Id.*

255 *Id.*

Another important difference between online service providers and traditional fiduciary duties relates to the level of fiduciary care. Traditional fiduciaries may advise their clients against doing something foolish besides avoiding to actively harm their clients.[256] In contrast, digital technology companies such as Google, Facebook, and Uber, do not have the same relationship to their users. They do not hold themselves out as taking care of end-users in general.[257] The nature of their duties depends on the *kind of business* they present to the public.[258] "Google and Uber may have a duty to protect our privacy in certain ways, but we do not expect them to warn us not to go on a particular trip."[259] "Facebook presents itself as helping us to connect with other people."[260] But we should not expect that Facebook has a fiduciary duty to warn us not to do something foolish. "Nor should we expect that Facebook has a duty to keep us from receiving links from our Facebook friends that are misleading or emotionally disturbing."[261] "In these contexts, their duty to protect us is quite limited."[262]

Therefore, Balkin concludes that the concept of information fiduciaries should exist between online companies and users, albeit in a more nuanced context. Online service providers should be thought of as "special-purpose information fiduciaries."[263] The level of duty imposed on them depends on the nature of their services.[264]

The service that Facebook provides to users, a forum on which data can be shared and stored, and its promotion of its services to users, imposes a duty on Facebook to that extent, which depends on what users would find unexpected or abusive. Data collecting by a third-party, as well as hacking private accounts, fall under unexpected and abusive actions by Facebook.[265] Even under the limited purview of Facebook's information fiduciary duty, data breaches and data

256 Balkin, *supra* note 124, at 1228 (citing *Cf.* Richard R.W. Brooks, *Knowledge in Fiduciary Relations*, *in* PHILOSOPHICAL FOUNDATIONS OF FIDUCIARY LAW at 225, 240 ("Fiduciaries . . . have not only duties of confidentiality and disclosure, but also duties to inquire, to inform, [and] to speak with candor . . . .").

257 *Id.*

258 Balkin, *supra* note 124, at 1225.

259 *Id.* at 1228.

260 *Id.*

261 *Id.* at 1228-29.

262 *Id.* at 1229.

263 *Id.*

264 Balkin, *supra* note 124, at 1229.

265 *See* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563 (2009).

collection by third-parties violates its information fiduciary, since users find this unexpected and abusive.[266] Included in this argument is that Facebook, as part of its information fiduciary duty, had to prevent its data from being disclosed and misused by Cambridge Analytica.[267] It should have held Cambridge Analytica to very stringent requirements for how they use the data and to whom they can disclose it to.[268] Facebook should have investigated Cambridge Analytica more closely.[269] Facebook's fiduciary obligations "run with the data," such that Facebook has a duty to make sure that whenever it allows another person or business to see, view, or employ Facebook's end-users' data; these persons and businesses must take on the same duties of trust and non-manipulation that Facebook itself must take on.[270]

Thus, Facebook should provide compensation to the affected users, since, as was previously established, digital data is considered property and there is a property law obligation to compensate users.

IV. GOVERNMENT CENSORSHIP OF SOCIAL MEDIA

There are examples of a ban on Facebook and other social media websites in other countries, particularly in autocratic regimes such China and Iran. In China, Facebook was blocked after the July 2009 political riots, because independence activists were using Facebook as part of their communications networks.[271] In Iran, after the 2009 election, due to fears of political unrest and a fear that opposition movements were being organized through Facebook, Facebook was blocked.[272] After four years, the ban was lifted, and access became

266 *See* Kiel Brennan-Marquez, Fourth Amendment Fiduciaries, 84 FORDHAM L. REV. 611, 611 (2015).

267 *See* Jack Balkin, *Stormy Daniels and Cambridge Analytica*, BALKINIZATION BLOG (Mar. 18, 2018), https://balkin.blogspot.com/2018/03/stormy-daniels-and-cambridge-analytica.html.

268 *Id.*

269 Jack Balkin, *Mark Zuckerberg Announces that Facebook is an Information Fiduciary*, BALKINIZATION BLOG (Mar. 21, 2018), https://balkin.blogspot.com/2018/03/mark-zuckerberg-announces-that-facebook.html.

270 *Id.*

271 *See* Kristina Zucchi, *Why Facebook is Banned in China and How to Access It*, INVESTOPEDIA, https://www.investopedia.com/articles/investing/042915/why-facebook-banned-china.asp, (last visited Sept. 28, 2018).

272 *See* Thomas Erdbrink, *Iran Bars Social Media Again After a Day*, N.Y. TIMES (Sept. 17, 2013), https://www.nytimes.com/2013/09/18/world/middleeast/facebook-and-twitter-blocked-again-in-iran-after-respite.html.

easier for Iranians.[273] However, this only lasted a day, as the next day, users lost access to social media websites.[274] Israel, too, in September 2016, agreed with Facebook to remove content that is deemed to be terrorist incitement.[275] During that period and the year before that, many terrorist networks were using Facebook to incite violence against Israelis and encouraged terrorists to attack Israelis.[276]

Besides banning social media websites for fear of political unrest, violence, hate speech, and terrorist incitement, there have been discussions of banning Facebook for children, and putting an age restriction on social media use.[277] Parents may be concerned that their children are viewing inappropriate material on social media that can affect their entire lives[278] stunting their academic and social growth.[279] Also, child use of social media can lead to online bullying, as it is easier for children to bully their peers solely online and with a free communication device that does not require seeing their victim face-to-face.[280] Aaron Saenz, a journalist for Singularity Hub, a news site dedicated to current media trends, in an article entitled, *Bullying Is Moving Online. Is There No Escape For Their Victims?*, pointed out that social media increases the potential effects of bullying, given the ease of spreading embarrassing information (such as a video or SMS) about a child to thousands of users in a matter of minutes.[281] This can turn into abuse and harassment of a child which can affect him or her their entire life.[282] Finally, a child's social skills can be slowed or stymied, since a child can be overly focused on interacting with others

273 *See id.*

274 *See id.*

275 *Facebook and Israel to work to monitor posts that incite violence,* GUARDIAN (London) (Sept. 12, 2016, 11:11 EDT), https://www.theguardian.com/technology/2016/sep/12/facebook-israel-monitor-posts-incite-violence-social-media?CMP=twt_gu.

276 *Id.*

277 *See* Mychelle Blake, *Should Social Networking Sites be Banned*, LOVETOKNOW *https://socialnetworking.lovetoknow.com/Should_Social_Networking_Sites_be_Banned* (last visited Sept. 28, 2018).

278 *See id.*

279 *See id.*

280 *See id.*

281 Saenz, Aaron. *Bullying Is Moving Online. Is There No Escape For Their Victims?*, SINGULARITYHUB (Oct. 23, 2010), https://singularityhub.com/2010/10/23/bullying-is-moving-online-is-there-no-escape-for-their-victims/.

282 *See id.*

online, and not real-person interactions, which can hurt the growth of social skills at a critical time in the child's life.[283]

A. Penalizing Facebook: Government Censorship of Facebook or Content Contained Therein

A remedy that would penalize Facebook for its lax attitude and policies that helped bring about the breach and collection of private data by a third party is federal government censorship of Facebook and its content. This involves the same analysis as the Nixon administration's attempted government censorship of the press in the 1970s, with an emphasis on the first amendment right to free speech; the essential question is whether there is a violation of the right to free speech should Facebook be censored.

Regarding censorship of the press, the U.S. Supreme Court in, *New York Times, Co. v. Sullivan*, held that the president does not have inherent power to stop the publication of news, as that would violate the First Amendment and destroy the fundamental liberty and security of the American people.[284] In its *per curium* opinion, the Court held that the government did not overcome the "heavy presumption against" prior restraint of the press in this case.[285] Justice Brennan, in a concurrence, argued that since publication of the stories would not cause an "inevitable, direct, and immediate event imperiling the safety of American forces," prior restraint was unjustified.[286]

I submit that the government has the constitutional right to ban Facebook because of the risk to users resulting from the data breach by Cambridge Analytica, and because of the risk of future breaches of this magnitude. There is no first amendment violation, because the internet has its own set of rules.[287] Because social media companies, such as Facebook, are publicly-traded companies, they generally are not within the purview of the First Amendment[288].[289] Facebook is not a public forum, does not shape the public discourse, and is thus not

283 *See id.*

284 New York Times Co. v. Sullivan, 403 U.S. 713 (1971).

285 *Id*. at 714.

286 *Id.* at 727.

287 *See* Stephany Bai, *The First Amendment and Social Media: The Rules Just Don't Apply*, TEEN VOGUE (Dec. 29, 2017), https://www.teenvogue.com/story/first-amendment-social-media.

288 The fact that Facebook is a publicly-traded company does not mean it is subject to First Amendment scrutiny. It is a corporation, not a governmental entity.

289 *See id*.

subject to the first amendment right to free speech.[290] Supreme Court dicta also supports this. In a 2017 case involving a North Carolina statute, which made it a felony for registered sex offenders to access social networking websites, the Court compared social media networks to traditionally public spaces like parks and streets;[291] but, that comparison was hardly dispositive of the issue of government censorship of social media sites, "especially considering that the court's decision rested primarily on the North Carolina law's expansive reach (the law constituted an absolute bar on mainstream means of communication for registered sex offenders)."[292] Indeed, the Court expressly stated, "this opinion should not be interpreted as barring a State from enacting more specific laws than the one at issue."[293] The federal government is thus constitutionally permitted to enact specific laws that ban or censure users from accessing social media sites.

V. CONCLUSION

This Note aims to present the key issues surrounding digital privacy in the 21st century with the forceful presence of social media in the lives of billions of people around the world. The solutions I propose will not completely eradicate the concerns that online platforms pose, but it is a framework from which to grow and expand as time marches forward. This is an evolving topic, and what is proposed in this Note may not be sufficient to solve the issues that digital users face tomorrow. But it is a start.

290 *See id*.

291 *See* Packingham v. North Carolina, 137 U.S. 1730 (2017).

292 Thomas Wheatly, *Why Social Media Is Not a Public Forum*, WASH. POST (Aug. 4, 2017), https://www.washingtonpost.com/blogs/all-opinions-are-local/wp/2017/08/04/why-social-media-is-not-a-public-forum/?utm_term=.e3b594c679b4.

293 *Packingham*, 137 U.S. at 1737.