

UNITED STATES DISTRICT COURT  
IN THE NORTHERN DISTRICT OF CALIFORNIA

SK

**EV 19 4591**

CIVIL ACTION NO: \_\_\_\_\_

✓  
Robert Zimmerman  
329 Sandpiper Lane  
Hampstead, NC 28443  
Tel # 910-232-8990  
Email: bobimmerman@usa.com

FILED  
99 AUG -7 2019 125  
SUSAN Y. BOONG  
CLERK, U.S. DISTRICT COURT  
NORTH DISTRICT OF CALIFORNIA

Robert Zimmerman, and )  
Uxor Press )  
Plaintiffs, )

v. )

COMPLAINT

Facebook, Inc., )  
Mark Zuckerberg, )  
Sheryl Sandberg, )  
John and Jane Does )

Defendants. )

WITH JURY TRIAL DEMAND

<b>TABLE OF CONTENTS</b>	<b>Page</b>
I. Jurisdiction and Venue.....	4
II. The Parties.....	7
III. Introduction to and Summary of the Unlawful, Willful and Reckless Misconduct of Facebook Defendants.....	9
IV. An Unregulated Facebook Threatens Everyone.....	17
V. Representative Foreign and Domestic Governmental Investigations into Facebook’s Use and Abuse of the Information Facebook has Collected from Its Users and Non-Users.....	33
VI. Facebook Defendants Conspiratorial Conduct and Admissions Regarding their Role in the Sabotage of the 2016 U.S. Presidential Election Cycle.....	42
VII. The Many Serious Dangers Inherent in Facebook’s Unregulated and Unaccountable, Monopolistic Business Model.....	80
VIII. Facebook’s Use of Its Users’ Information as an Extremely Valuable Asset When Negotiating Deals with Third Parties to Gain Unfettered Access to It.....	88
IX. Russian "Active Measures" Deployed to Sabotage the 2016 U.S. Presidential Elections Using the Facebook Platform as Set Out in the Special Counsel’s Redacted Report.....	102
X. Causes of Action.....	110
Count One- Violation of the Computer Fraud and Abuse Act.....	110
Count Two- Unjust Enrichment.....	112
Count Three-Violation of Constitutional Rights.....	113
Count Four- Breach of the Implied Covenant of Good Faith and Fair Dealing.....	123
Count Five-Invasion of Privacy – Public Disclosure of Private Facts.....	125

Count Six-Civil Conversion.....	128
Count Seven-Negligence and Gross Negligence.....	130
Count Eight-Negligent and/or Fraudulent Misrepresentation.....	134
Count Nine-Breach of Contract.....	136
Count Ten-Willful Infliction of Emotional Distress.....	138
Count Eleven-Common Law Civil Conspiracy.....	139
Count Twelve-Deceit by Concealment.....	142
Count Thirteen-Fraud.....	150
Count Fourteen- Willful Misrepresentation.....	151
Count Fifteen-Civil RICO Conspiracy.....	153
Count Sixteen-Violation of the Stored Communications Act.....	156
Count Seventeen-Violation of California’s Computer Data & Fraud Act.....	160
Count Eighteen-Violations of California’s Unfair Competition Law.....	161
XI. Prayer for Relief.....	166
XII. Demand for Jury Trial.....	167

## I. JURISDICTION AND VENUE

1. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d), as the amount in controversy exceeds \$75,000.00 and supplemental jurisdiction pursuant to 28 U.S.C. §1367.
2. This Court also has diversity jurisdiction pursuant to 28 U.S.C. §§ 1331 1332 because Plaintiffs reside in North Carolina, and Facebook Defendants (hereafter “FB” or “FB Defendants “) reside and/or do business in California and North Carolina.
3. This action is also brought pursuant to the U.S. Constitution, as authorized by Article III, section 2, which extends federal judicial power to all cases arising in equity under the U.S. Constitution.
4. This grant of equitable jurisdiction requires Article III courts to apply the underlying principles of the U.S. Constitution to new circumstances unforeseeable by the Framers off the Constitution.
5. An actual controversy has arisen and exists between Plaintiffs and FB Defendants because FB Defendants have placed Plaintiff Zimmerman in a dangerous situation and continue to infringe upon Zimmerman’s constitutional rights and have abrogated their duty of care to ensure Zimmerman’s reasonable safety, among other violations of federal and state law.
6. The U.S. Constitution recognizes and preserves the fundamental right of citizens to be free from such actions that harm life, liberty, and property, including our nation’s election systems, privacy and free speech (especially political speech), which are critical to

Zimmerman's rights to life, liberty, and property and which have been, and continue to be, harmed by FB Defendants

7. The above named inherent and inalienable rights reflect the bedrock societal guaranty inherent in the U.S. Constitution, which is to protect citizens and posterity from unconstitutional infringement upon basic freedoms and human and natural rights.
8. The rights to life, liberty, and property have evolved and continue to evolve as technological advances, as here, pose new challenges to these fundamental rights and as new insights reveal discord between the Constitution's central protections and the conduct of government and private parties.
9. This case is likely one of the first filed in this Court that addresses the relationship between the First Amendment and the Internet-based FB communications platform.
10. A fundamental principle of the First Amendment is that all persons have unfettered access to places where they can speak and listen, and then, after reflection, speak and listen once more. A basic rule is that a street or a park is a quintessential forum for the exercise of First Amendment rights. See *Ward v. Rock Against Racism*, 491 U. S. 781, 796 (1989).
11. FB often brags that it offers its users a free facility for communications of all kinds. See *Reno v. American Civil Liberties Union*, 521 U. S. 844, 868 (1997).
12. Among many other promises, FB maintains that its users can debate religion and politics.
13. All fifty states, thousands of cities and towns, and almost every elected U.S. official have FB accounts.

14. Also, federal courts always have the authority to determine whether they have the jurisdiction to hear a particular case. *United States v. Ruiz*, 536 U.S. 622, 628 (2002) (citing *United States v. Mine Workers of Am*, 330 U.S. 258,291 (1947)). This Court also has original jurisdiction over this action pursuant to 28 U.S.C. §1331 as this action involves allegations of violations of the U.S. Constitution.
15. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391(e) because the FB Defendants are subject to personal jurisdiction in this judicial district because they reside and/or do business in this district.
16. Venue is also proper in this District pursuant to 28 U.S.C. §1391(b)(2) because a substantial part of the conduct and events giving rise to Plaintiff's claims occurred in this District.
17. Venue is also proper because a substantial part of the conduct giving rise to Plaintiff's claims occurred in or emanated from this District and the relevant terms of Plaintiff's contracts with FB provide that the exclusive venues for litigating any claim with FB are either the United States District Court for the Northern District of California or a state court located in San Mateo County. These non-negotiable, FB adhesion contracts also provided that all claims that might arise between the user and FB would be governed by the laws of California, without regard to conflict-of-law provisions.
18. The FB venue provision provides an additional reason that venue is proper in this District. That choice-of-law provision establishes that California law applies to Plaintiff's claims.

19. Moreover, with regard to the choice of law, FB's "Terms of Service" (formerly known as the "Statement of Rights and Responsibilities") contain (and have always contained) a forum selection provision that mandates the resolution of any claim, arising either out of the "Terms of Service" or a person's use of FB, exclusively in the U.S. District Court for the Northern District of California and provides that FB users submit to the personal jurisdiction of those courts to litigate those claims.
20. In addition, the FB "Terms of Service" contain (and have contained since at least April 26, 2011) a California choice-of-law provision, which provides that California law applies to "any claim that might arise between" a user and FB.
21. Plaintiffs could not have brought forth the entirety of their claims until whistleblower Christopher Wylie testified to the U.K. Parliament in 2018 that on or about July 2014 FB's engineers assisted Cambridge Analytica with its plundering of the personal information of nearly a hundred million FB users.

## **II. THE PARTIES**

22. Plaintiffs repeat and re-allege all preceding and following paragraphs as if fully set forth herein.
23. Plaintiff, Robert Zimmerman ("Zimmerman"), is nearly 79 years old, a registered voting voter and veteran who resides in Hampstead, North Carolina.

24. He has written three political books that set out progressive agendas for the U.S.: *Metacapitalism* (1985), the *American Challenge* (2005) and *Common Sense* (2016) available online free of charge.
25. Zimmerman was also a grassroots Democratic candidate for the U.S. Senate, finishing second of eight candidates in a Democratic primary, losing to a multi-term, favorite son incumbent.
26. While campaigning, Zimmerman was arrested for trespassing in a downtown public park and at a state fair for distributing copies of the U.S. Constitution and his campaign brochure to prospective voters and was found not guilty.
27. Plaintiff Uxor Press is a small unincorporated publishing business, 100% owned by Zimmerman. Uxor Press published the books listed above and a few others.
28. Zimmerman's political activities and books demonstrate that he has been deeply involved in U.S. politics for over three decades and has been severely damaged directly and indirectly by the anti-democratic conspiratorial and non-conspiratorial actions and inactions of FB Defendants.
29. FB, Inc. is incorporated in the State of Delaware. It has principal offices at 1601 Willow Road and at 1 Hacker Way, both in Menlo Park, California 94025.
30. FB Defendant Mark Zuckerberg (hereafter "Zuckerberg" or "Mark Zuckerberg" or "FB Defendants" or "FB"). He is FB's co-founder and Chief Executive Officer at all relevant times.



31. FB Defendant Sheryl Sandberg (hereafter “Sandberg” or “Sheryl Sandberg” or “FB Defendants” or “FB” is FB’s Chief Operating Officer (“COO”).

32. Named and unnamed unserved John and Jane Does.

### **III. INTRODUCTION TO AND SUMMARY OF THE , WILLFUL AND RECKLESS MISCONDUCT OF FB DEFENDANTS**

33. Plaintiffs incorporate by reference all paragraphs contained throughout this Complaint as if fully set forth herein.

34. FB, Inc. (hereafter “FB”) is arguably the world’s most powerful corporation, with a global audience of some 2.2 billion people, who use its platform to message with each other, for local, nation and international news and many other purposes.

35. FB Defendants, (hereafter referred to collectively as FB or Facebook, have used and continue to use the FB platform and their immense wealth to transform the world, particularly the U.S. in ways that only the FB can control, including the successful sabotage of the 2016 presidential election cycle and the prospective introduction of FB’s own international currency under the aegis of Swiss law.

36. Hundreds of millions of FB users obtain most of their news by from the FB platform and that news is selected by FB without any recompense by FB to the legitimate global press.

37. FB does not any of deploy standard journalistic fact checking safeguards to avoid fake news and other forms of misleading propaganda such as that deployed by Russian operatives, the Trump Campaign, Cambridge Analytica, Robert Mercer and others during, and now after, the 2016 U.S. presidential election cycle.

38. FB violated Plaintiff Zimmerman's First Amendment rights by first granting him and his publishing company unfettered access to the FB platform and then unlawfully revoking that access causing Plaintiffs severe economic harm and other injuries.
39. After revoking Plaintiffs access, FB has admitted that they granted unfettered access to FB user information, such as Plaintiffs' had supplied to FB in order to gain unfettered access to the FB platform, to numerous third parties without Plaintiff's knowledge or consent and in doing so, FB caused billions of FB users' privacy to be invaded and inflicted severe economic harm and other injuries on them.
40. In 2018, investigative journalists discovered that a British political consulting and information mining firm called Cambridge Analytica unlawfully obtained the FB user' information of many millions of FB users, possibly including that of the Plaintiffs, and used it in various ways together with others to successfully sabotage the 2016 U.S. and the 2020 presidential election cycles in favor of candidate Donald J. Trump, who later became a subject of a Department of Justice ("DOJ") appointed Special Counsel's investigation into that sabotage.
41. Cambridge Analytica's unlawful misappropriation and unlawful use of FB user information was one of many plunders and unlawful uses of FB user' information.
42. Since approximately 2008, without the knowledge or permission of their users, FB encouraged and allowed numerous third-parties to download FB user' information; other plunderers were not FB authorized.

43. FB also traded or sold unfettered access to Plaintiff's users' information to numerous individuals, businesses and governmental agencies,
44. These investigative reporter revelations have shown that FB is far more than a supplier purportedly free access to an Internet-based communications platform. FB is also one of the world's largest sellers of advertising space, an information brokerage and surveillance firm and derives billions in annual profits from these activities.
45. FB, having recognized that its users' public and private information is incredibly valuable, set about collecting, storing and supplementing and aggregating that information and then selling and trading unfettered access to that information to its business partners and numerous other third parties.
46. If FB had proceeded lawfully, instead of unlawfully as it did, as a seller of advertising space and an information brokerage and surveillance firm, it would have, at a minimum, obtained the consent of its users to sell and trade, aggregate and supplement its users' information, but FB never did.
47. It's likely that the vast majority of FB's billions of users are not aware of how FB is exploiting their information and the dangers and other problems that they may encounter as a result of FB's exploitive activities.
48. FB's deceptive, willful, reckless and unlawful conduct violated the contractual promises and public pronouncements that it would protect the privacy of its users' information and was recently fined \$ five billion by the Federal Trade Commission ("FTC") for such user privacy violations.

49. To encourage prospective users/communicators to join and engage with each other on its Internet-based communication platform, FB misled prospective users into believing that they controlled their FB user' information through certain privacy settings and other FB tools.
50. But, contrary to FB's express promises, these privacy settings and other tools did not prevent access by numerous third-parties.
51. FB also manipulated FB users' default privacy settings. In April 2010, FB unilaterally changed users' default "Profile Privacy Settings" so that the default settings indiscriminately shared FB user' information with third parties. This change sparked the concerns of privacy advocates and ultimately the FTC.
52. Reasonably believing in FB's user information privacy promises , Plaintiffs shared their FB user' information and messages with their FB "Friends." FB "Friends" are persons and entities that are FB users that have agreed to communicate with Plaintiffs on the FB platform.
53. The comprehensiveness of the FB user' information, unavailable to traditional sellers of advertising space, is what makes it so valuable to advertisers and others who wish to personally target FB users with their messages and gives FB a substantial competitive edge over them.
54. It is the atypical way that FB collects, analyzes and deploys FB user' information that inflicts a novel and more invasive kind of harm than typical information breaches.

55. FB's aggregation of its users' information allows third parties and FB to make that FB user' information public and/or share it with third parties and connect it to specific users, by name, contrary to FB's explicit pledge not to sell FB user' information to advertisers or share it with third parties.
56. The fundamental segments of a FB users' information profile are pictures, phone numbers, email addresses and the kind of corroborating personal information used for passwords and security questions are essential ingredients for identity theft and other malicious online activity.
57. Information access and processing experts agree that this aggregated information makes people much more vulnerable to voter fraud, medical fraud, phishing, and other identity-based harms.
58. The harm is not limited to identity theft. The ability to analyze and deanonymize FB user' information allows third parties to personally and psychologically target FB users with greater precision, a technique now called psychographic marketing.
59. For example, Cambridge Analytica exploited FB users' information to target individual voters with content tailored to their predicted psychological proclivities.
60. FB and other information brokers compile dossiers on FB users based on this aggregated content. The dossiers make assumptions about users' health, financial risk, employability and other factors

61. Information brokers like FB then make that information accessible to third parties, including advertisers, hackers and political subversives to target people based on analyses of their temperament and vulnerabilities.
62. FB has repeatedly professed remorse for willfully violating its users' privacy.
63. Following entry of the 2012 FTC "Consent Decree," Zuckerberg stated, "...we've made a bunch of mistakes [intentional conduct that produced many billions in profit for FB]."
64. Zuckerberg then assured FB users that FB was committed to providing its users with "complete control over who they share with at all times." See Zuckerberg's pledge at, *Our Commitment to the Facebook Community*, FB Newsroom (Nov.29, 2011), <https://newsroom.fb.com/news/2011/11/our-commitment-to-the-facebookcommunity/>.
65. Zuckerberg added, "This means we're making a clear and formal long term commitment to do the things we've always tried to do and planned to keep doing, giving you [FB users] tools to control who can see your information and then making sure only those people you intend can see it."
66. Since the Cambridge Analytica FB user' information plundering scandal was exposed, Zuckerberg has continued apologizing for FB's unlawful activities, usually calling that willful and for profit unlawful activity a "mistake" but never offering FB users any redress for FB's unlawful conduct.
67. For example, on April 18, 2018, Zuckerberg admitted, "We didn't focus enough on preventing abuse and thinking through how people could use these tools to do harm as well. That goes for fake news, foreign interference in elections, hate speech, in addition

to developers and information privacy. We didn't take a broad enough view of what our responsibility is, and that was a huge mistake. It was my mistake.”

68. The time for pro forma apologies by FB Defendants has long since passed.

69. Now, only judicial process, such as this and numerous other lawsuits, can redress those injured by FB's malicious and reckless unlawful conduct.

70. Zimmerman and his solely-owned publishing business Uxor Press bring this action seeking recovery for injuries suffered as a result of the willful, unconstitutional, conspiratorial, reckless, outrageous, unlawful and possibly treasonous conduct of FB and also seeks injunctive relief that to forestall and deter FB and others from such unlawful and improper conduct in the future.

71. On March 8, 2019, Senator and presidential candidate Elizabeth Warren proposed breaking up FB as has FB's co-founder Chris Hughs as well as numerous civil lawsuits foreign and domestic governmental investigations involving FB's alleged monopolistic and other unlawful conduct, including FB's information-sharing-agreements with third parties and participation in the sabotage of the U.S. 2016 presidential elections.

72. Only a few days after Senator Warren unveiled her FB breakup proposal, FB pulled her political ads from its platform, to a far lesser degree, the very same sort of malicious, First Amendment defying censorship FB Defendants deployed against Plaintiffs.

73. In ever-increasing numbers, consumers, lawmakers, regulatory agencies domestic and foreign, investors and private citizens the world over are increasingly concerned about FB's unlawful use of its monopoly power.

74. Complaints against FB include FB's failure to safeguard FB user' information, FB's failure to protect its users from, among other things, hate speech, terrorist propaganda and recruitment activity, child abuse, Russian political propoganda, U.S. election sabotage, all sorts of disinformation and live footage of violent acts.
75. FB has agreed to hand over the identification information of French FB users suspected of hate speech on its platform to French judges but has entirely ignored a 2012 "Consent Decree" it signed with the FTC. More on the "Consent Decree" below.
76. Among other serious unlawful activities, FB willfully breached FB's contracts and promises with Plaintiffs by permitting third parties like Cambridge Analytica, Russian intelligence agents and operatives, Robert Mercer and the Trump Campaign to willfully exploit FB's lax to non-existent user privacy protections.
77. Contrary to FB's purported mission to connect the entire world, FB blocked Plaintiffs business and personal accounts and by so doing violated Zimmerman's First Amendment right to publish his non-violent, pro-democracy, political views on FB's platform and market his political and non-political books on FB's platform, and in so doing knowingly, recklessly and unlawfully violated Zimmerman's free speech rights and his constitutionally-protected right to participate in free and fair elections as well as his Fourth Amendment privacy rights by willfully allowing third-parties to access his FB user information without seeking Plaintiff's authorization and without his knowledge.
78. As late as July 2019, a FB executive in charge of global information testifying before Congress could not or would not answer a congressman's question regarding why Al Qaeda



is still allowed to recruit terrorists using the FB platform.

79. The constitutional violations, conspiratorial and other tortious and criminal conduct of FB includes:

- Direct and indirect participation in a racketeering enterprise. See Count Fifteen.
- Willful, promised and repeated failure to protect and not make available to third parties Plaintiff's user' information that Plaintiffs had entrusted to it;
- Blocking Plaintiff's access and use of his personal and business accounts;
- Active participation in the sabotage of the 2016 U.S. presidential elections by facilitating the Trump Campaign's use of Plaintiff's plundered FB user' information and communications to sabotage of the 2016 U.S. presidential elections, primary and general.
- Failure to block Cambridge Analytica from the theft and use Plaintiffs' FB user' information and that of nearly a hundred million other FB users' information to help sabotage the 2016 U.S. presidential elections.

#### **IV. AN UNREGULATED FB THEATENS EVERYONE**

80. Plaintiffs repeat and re-allege all preceding and following paragraphs throughout this Complaint as if fully set forth herein.

81. FB and one man, FB's CEO Mark Zuckerberg, and one woman, FB's COO Sheryl Sandberg, without any effective checks on their conduct, have amassed monopolistic power and have used that power in a intentionally deceptive, reckless and unlawful manner that endangers and negatively impacts the quality of the life and constitutional rights of

Plaintiffs and billions of other FB users and non-users, going so far as to recently propose the creation of its own international currency that would be based in Switzerland and could likely threaten the stability of the global financial system and markets and the U.S. governments., as well as many others. More on FB's proposed currency below.

82. FB Defendants have played the principle role in accelerating the transformation of America and other nations from the age of information to the age of disinformation, a transformation that tears at the very fabric of the democratic ideals envisioned by America's Founders.
83. Other businesses like *Fox News* are also culpable, but none of them has anything like the global reach (billions of FB users), financial and technological resources, unregulated monopolistic power, and seemingly boundless ambition to trample on our rights to free speech, free and fair elections and our right to privacy as does FB.
84. FB has devised rules of the road that benefit only FB at the expense of its users' privacy and safety, always surveilling its users and treating them in whatever way FB deems most advantageous to FB unrestrained by any ethical norms and only a few, and mostly ineffective government imposed rules and regulations.
85. The former head of FB's information science team described FB's user tracking and surveillance to a microscope that allows FB to examine its users' social behavior with a degree of intensity never previously available and to run undetected experiments on its billions of users without regard to their privacy and safety and for no social purpose whatsoever other than advancing FB's monopolistic and political power.

86. Another member of the information science team said “Anyone on [that] team could run a test. They’re always trying to alter people’s behavior.”
87. As FB gains greater and greater monopolistic market reach and financial and political power by, among other things, tracking its user’s activities and shaping the news its users’ see, the threat to our democracy grows ever greater as occurred when FB willfully participated with Russian operatives, the Trump Campaign, Robert Mercer, Cambridge Analytica and others in the sabotage of the primary and general 2016 U.S. presidential elections.
88. Shortly after FB offered a small portion of its stock to the public, FB amassed over a billion dollars in profit and paid no income tax, actually receiving an approximately \$400 million tax deduction and/or refund by writing off the value of the stock options it conferred on certain of its executives.
89. In 2018, FB spent over \$22 million to protect Zuckerberg from harm and hardly a pittance, if anything, to protect Plaintiffs and billions of other FB users and non-users that it was willfully placing in danger.
90. The many dangers, past, present and future FB has inflicted, and will continue to inflict, on its users and non-users are many. Even so, FB has effectively established itself in the everyday life of millions of Americans, which provides all the more reason for this Court to act to thwart the very real dangers and other perils that FB users and non-users face from an unregulated FB.

91. In sum, among many perilous and otherwise damaging activities the virtually an unregulated FB routinely aids and abets includes:

- Election rigging;
- Terrorist activity;
- Organized immigration crime.
- Slavery trafficking.
- Extreme and revenge pornography;
- Incitement of violence, hate crime, harassment, intimidation, bullying, trolling and Cyberstalking;
- Sale of illegal goods and services, such as drugs and assault weapons;
- Content unlawfully uploaded to and from prisons;
- Sexting and distributing indecent or sexual images of children under the age of 18;
- Children accessing pornography and other inappropriate material, including children under 13 using dating applications;
- Child sexual exploitation and abuse by pedophiles;
- Distribution of enemy and adversary propaganda and disinformation;
- Advocacy of self-harm, female genital mutilation and suicide.

92. As late as July 2019, FB, Twitter, Google and other platforms say they are actively collaborating to fix the above-listed problems.

93. These multibillion dollar corporations claim they have formed a group through which they are actively collaborating to remedy the above-listed problems, which is nothing but an

egregious deception as the so-called group has no budget, no assigned full time employees and no physical meeting place, no discrete short or long term measurable or even non-measurable specific objectives and no established timeframe for accomplishing anything.

94. The U.S. government, much like it did when it failed to assert the dangers of smoking, has entirely failed to take the actions necessary to protect Americans from an unregulated FB.

95. Most Americans are unaware of the very real dangers an unregulated FB poses, though some Americans were successfully recruited by Al Qaeda's use of the FB platform. See, *Zucked: Waking Up to the FB Catastrophe*, (2019), by Roger McNamee, a large FB shareholder.

96. An unregulated FB, among other nefarious activities, is used to spread hate speech, to abuse and bully and to undermine our democratic values and limit legitimate debate.

97. The impact of unregulated and harmful FB messaging is particularly damaging for children and that activity is widespread on FB.

98. In 2018 there were over 18.4 million referrals of child sexual abuse material to the National Center for Missing and Exploited Children.

99. Child sex offenders use FB to view and share child sexual abuse material, recruit children for sexual abuse and broadcast images of the sexual abuse of children.

100. The prevalence of anti-democratic propaganda messaging on FB threatens our national security and thus the physical safety of every American and is obviously unacceptable.

101. FB is used by terrorists to recruit vulnerable people with propaganda designed to radicalize and incite violence against the U.S. and elsewhere.
102. Terrorist groups also use FB to broadcast live terrorist attacks.
103. Dangerous opioids are marketed and sold on FB.
104. Hostile actors increasingly use FB to spread disinformation to undermine our democratic values the rule of law.
105. FB uses sophisticated algorithms that send FB users to ‘echo chambers or ‘filter bubbles, where FB users are presented with disinformation instead of seeing a range of voices and opinions. This ensures that FB users do not see messaging that runs contrary to the disinformation FB helps broadcast for Russia and other U.S. adversaries.
106. Criminal gangs use FB to promote gang culture and incite violence. This, together with the illegal sale of weapons to young people online, is a contributing factor in the dramatic rise of lethal gang violence on America’s streets.
107. FB is used to harass, bully or intimidate people in vulnerable groups or in public life. The President prefers Twitter and *Fox News*.
108. FB increasingly exposes young adults and children to all sorts of harmful content that serves to induce violent behavior, self-loathing and harm and suicide.
109. FB has worked strategically to maintain its monopolistic policies and practices, which include willful and numerous violations of constitutional and antitrust law.

110. Columbia Law School professor Tim Wu observes in his book *The Curse of Bigness* has said: “To think of monopolies and oligopolies as worrisome only if they charge high prices is a narrow perspective.”

111. In practice, monopolistic product pricing is only one form of harm that giant corporations like FB often inflict.

112. FB’s market dominance and technical knowhow allows FB to behave in dangerous ways.

113. Without seeking permission from its users, FB collects and uses for its own purposes the public and private FB user’ and non-user’ personal information of billions of people, and businesses and governments, including Plaintiffs.

114. FB then uses that information in various ways to increase its advertising and other revenue intake and profitability, including selling targeted advertising, selling targeted product and life-style research and selling FB user information and its technological expertise to aid and abet the rigging of political elections.

115. FB has an extensive history of failures to protect it user’s privacy.

116. For example, in 2007 FB implemented an information tracking computer program called Beacon, which lifted information about FB user’s purchases and activities from other platforms and websites and then posted that information to FB’s “NewsFeed” without obtaining FB user’ approval.

117. Weeks after Beacon’s introduction, FB users responded by signing a petition demanding that FB stop its Beacon activities, citing concerns over privacy.

118. In response, FB created an “opt-out” from the service. Zuckerberg commented, “[w]e simply did a bad job with this release, and I apologize...” (one of numerous FB Defendants’ admissions against interest.)

119. Nineteen FB users, unsatisfied with FB’s response to their complaints, sued FB for violations of various state and federal privacy statutes, and sought damages and a variety of equitable remedies. FB settled certain of these lawsuits for \$9.5 million.

120. The terms of the settlement included FB agreeing to terminate its use of Beacon and funding a new charity organization called the Digital Trust Foundation whose mission was to “fund and sponsor programs designed to educate users, regulators and enterprises on critical issues relating to protection of identity and information online through user control, and the protection of users from online threats.”

121. Despite agreeing to terminate its use of Beacon, FB’s counsel stated that nothing in the settlement agreement precluded FB from reinstating FB’s use of Beacon after changing its name.

122. In 2008, FB introduced Open ID, an application that gave FB users a means to log on to other websites with their FB credentials.

123. FB also made its “Like” button available on other websites, further blurring the lines of privacy and allowing for widespread tracking of a person’s web browsing history, even for non-FB users.



124. One year after FB's launch of Open ID, FB changed its default settings to make its user's profiles public by default. FB users objected. Even so, but it took FB five years to restore the previous default settings.

125. In December 2009, without warning or obtaining their users' approval, FB changed its platform so that certain information that its users had designated as private was made readily available to third parties.

126. FB represented that third party applications installed by FB users would have access only to FB user' information needed to operate, when, in fact, the third party applications and their developers could access most FB user's information.

127. FB also told FB users they could restrict the sharing of their FB user' information to FB "Friends Only." However, selecting "Friends Only" did not prevent FB user's information from being accessed by third parties. See, *Lane v. FB Inc.*, 696 F.3d 811 (9th Cir. 2012). See also *Transcript of Fairness Hearing* dated February 26, 2010 and *Lane v. FB, Inc.*, Civ. No. C 08-3845 (ND Cal.) After FB users protested, Zuckerberg apologized for what he called his "mistake" and promised to do better.

128. Had the CEO of any other large corporation made what Zuckerberg deemed his "mistake," his board and shareholders would have fired that person. But Zuckerberg, who owns the controlling voting shares in FB, is uncontrollable by FB shareholders or, so it seems by any governmental regulatory agency, the FTC excepted, or the DOJ.

129. As long as FB had rivals, the fear of losing its users somewhat restrained FB's behavior.

130. But as FB's growth has surged, FB, following in the footsteps of other current and previous monopolies, has stepped up its purchase of competitors, and with competitive pressure no longer a FB concern, FB has deceptively, recklessly and willfully ignored the privacy promises they had contracted with its users to uphold because now FB users have no viable alternative to FB.

131. In ever more deceptive ways, FB continues to violate its non-negotiable privacy and policy practices.

132. FB developed plugin algorithms called "Like" and "Share" buttons that it licenses to website owners. The licenses require third party website owners to install the plugin algorithms on their websites, which opens a pathway of communication between FB user's devices and FB's user' information repositories.

133. FB had promised it would not use this licensing pathway to conduct commercial surveillance and later reneged on that promise.

134. Having taken the FB licensing pathway promise as gospel, CNN, the *New York Times*, the *Wall Street Journal*, *Slate* and ABC were among the first companies to sign up for the plugins.

135. However, in June 2014, FB publicly reversed course by announcing it would use its licensing algorithm plugins as installed on third party websites to surveil consumer behavior.

136. By then, FB's licensing algorithm was installed on millions of websites and mobile applications and rapidly spread like an undetected, highly infectious, plague.

137. These days, all a person has to do is visit a page with a “Like” button, and FB, without authorization, collects, stores and aggregates your public and private information, such as what you’re buying or what you’re reading or where you’re traveling.

138. FB’s monopolistic conduct negatively impacts billions of people and businesses, including Plaintiff’s.

139. FB uses its market dominance and unlawfully obtained information resources to undercut their competitors in the advertising market because its purloined consumer information allows it to target FB users’ preferences and behavior than other sellers of advertising can.

140. For example, the *New York Times* may know which of its online readers have clicked on its health-related content. But FB knows which *Times* health-content readers vacation in Florida, shop for Nike shoes and read workout blogs because its widespread coding gives it the capability to track people all over the Internet and connect that online activity to their FB user’ information repositories.

141. Thus, the *Times* cannot effectively compete with FB’s illicitly gained edge in the advertising market. Moreover, the *Times* pays most its content producers, while FB merely steals the information that it needs.

142. This is one big reason why newspapers and other online publishers are experiencing financial difficulty. While FB continues racking up record profits, it poses an ever-increasing threat to our fragile democracy, to fair competition, to privacy and free speech, to the rule of law and to free and fair elections.

143. One powerful remedy to FB's monopolistic policies and practices is the U.S. Sherman Antitrust Act of 1890, written at the height of the Gilded Age to confront the out-of-control growth of concentrated power in business and the anti-competitive conduct of monopolies.
144. FB is in violation of the Sherman Antitrust Act because it has harmed countless millions of people and businesses by deploying monopolistic business practices and policies to restrict competition and relentlessly continues to expand its monopoly market power with its willfully reckless, deceptive and unlawful conduct.
145. In the wake of increasingly expressed public anger, Zuckerberg announced a new privacy vision for FB, a willfully deceptive, self-serving vision that entirely fails to address any of FB's monopolistic policies and practices.
146. Calls for holding FB accountable for its unlawful conduct include Senator Elizabeth Warren and the *New York Time*'s Kevin Roose, who favor breaking up FB.
147. Senator Warren also called for reclassifying FB as a public utility.
148. Meanwhile, much like the monopolists of the Gilded Age, Zuckerberg insists that FB is only interested in the progress of civilization, in his words "bringing the world closer together."
149. Unfortunately, what unaccountable monopolies typically do is tear the world apart, not closer together as its election rigging and broadcast of hate speech shows.
150. Throughout history, unregulated and unaccountable monopolies like FB have produced economic inequality, stifled innovation and created widespread public anger, a

condition that has enabled anti-democratic authoritarian governments, a condition remarkably similar to those now tearing at the roots of America's already fragile democracy.

151. Fortunately, the last Gilded Age taught us something about how to control monopolists.

152. It won't happen under President Trump and the Republican-dominated Congress, but certain of the President's 2020 challengers are making breaking up monopolies like FB a central part of their appeal to voters and before that our judiciary and regulatory agencies may take appropriate action.

153. Historically, the American electorate voted for trustbusting, anti-monopolists like Theodore Roosevelt who promised to and did enforce the Sherman Antitrust Act.

154. In 2018, the FTC announced a prospective large fine against FB, large but only chump change in view of FB's vast financial resources and its willful violations of the 2012 "Consent Decree" FB signed with the FTC but has not honored. Following are the 2012 FTC Orders FB has ignored:

**Part I. IT IS ORDERED** that Respondent and its representatives, in connection with any product or service, in or affecting commerce, shall not misrepresent in any manner, expressly or by implication, the extent to which it maintains the privacy or security of covered information, including, but not limited to:

- A. its collection or disclosure of any covered information;
- B. the extent to which a consumer can control the privacy of any covered information maintained by Respondent and the steps a consumer must take to implement such controls;
- C. the extent to which Respondent makes or has made covered information accessible to third parties;
- D. the steps Respondent takes or has taken to verify the privacy or security protections that any third party provides;

E. the extent to which Respondent makes or has made covered information accessible to any third party following deletion or termination of a user's account with Respondent or during such time as a user's account is deactivated or suspended; and

F. the extent to which Respondent is a member of, adheres to, complies with, is certified by, is endorsed by, or otherwise participates in any privacy, security, or any other compliance program sponsored by the government or any third party, including, but not limited to, the U.S.-EU Safe Harbor Framework.

**Part II. IT IS FURTHER ORDERED** that Respondent and its representatives, in connection with any product or service, in or affecting commerce, prior to any sharing of a user's nonpublic user information by Respondent with any third party, which materially exceeds the restrictions imposed by a user's privacy setting(s), shall:

A. clearly and prominently disclose to the user, separate and apart from any "privacy policy," "data use policy," "statement of rights and responsibilities" page, or other similar document: (1) the categories of nonpublic user information that will be disclosed to such third parties, (2) the identity or specific categories of such third parties, and (3) that such sharing exceeds the restrictions imposed by the privacy setting(s) in effect for the user; and

B. obtain the user's affirmative express consent.

Nothing in Part II will (1) limit the applicability of Part I of this order; or (2) require Respondent to obtain affirmative express consent for sharing of a user's nonpublic user information initiated by another user authorized to access such information, provided that such sharing does not materially exceed the restrictions imposed by a user's privacy setting(s). Respondent may seek modification of this Part pursuant to 15 U.S.C. §45(b) and 16 C.F.R. 2.51(b) to address relevant developments that affect compliance with this Part, including, but not limited to, technological changes and changes in methods of obtaining affirmative express consent.

**Part III. IT IS FURTHER ORDERED** that Respondent and its representatives, in connection with any product or service, in or affecting commerce, shall, no later than sixty (60) days after the date of service of this order, implement procedures reasonably designed to ensure that covered information cannot be accessed by any third party from servers under Respondent's control after a reasonable period of time, not to exceed thirty (30) days, from the time that the user has deleted such information or deleted or terminated his or her account, except as required by law or where necessary to protect the FB website or its users from fraud or illegal activity. Nothing in this paragraph shall be construed to require Respondent to restrict unfettered access to any copy of a user's covered information that has been posted to Respondent's websites or services by a user other than the user who deleted such information or deleted or terminated such account.

**Part IV. IS FURTHER ORDERED** that Respondent shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive privacy program



that is reasonably designed to (1) address privacy risks related to the development and management of new and existing products and services for consumers, and (2) protect the privacy and confidentiality of covered information. Such program, the implementation of which must be documented in writing, shall contain controls and procedures appropriate to Respondent's size and complexity, the nature and scope of Respondent's activities, and the sensitivity of the covered information, including:

A. the designation of an employee or employees to coordinate and be responsible for the privacy program.

B. the identification of reasonably foreseeable, material risks, both internal and external, that could result in Respondent's unauthorized collection, use, or disclosure of covered information and an assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this privacy risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management, including training on the requirements of this order, and (2) product design, development, and research.

C. the design and implementation of reasonable controls and procedures to address the risks identified through the privacy risk assessment, and regular testing or monitoring of the effectiveness of those controls and procedures.

D. the development and use of reasonable steps to select and retain service providers capable of appropriately protecting the privacy of covered information they receive from Respondent and requiring service providers, by contract, to implement and maintain appropriate privacy protections for such covered information.

E. the evaluation and adjustment of Respondent's privacy program in light of the results of the testing and monitoring required by subpart C, any material changes to Respondent's operations or business arrangements, or any other circumstances that Respondent knows or has reason to know may have a material impact on the effectiveness of its privacy program.

**Part V. IT IS FURTHER ORDERED** that, in connection with its compliance with Part IV of this order, Respondent shall obtain initial and biennial assessments and reports ("Assessments") from a qualified, objective, independent third party professional, who uses procedures and standards generally accepted in the profession. A person qualified to prepare such Assessments shall have a minimum of three (3) years of experience in the field of privacy and data protection. All persons selected to conduct such Assessments and prepare such reports shall be approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, in his or her sole discretion. Any decision not to approve a person selected to conduct such Assessments shall be accompanied by a writing setting forth in detail the reasons for denying such approval. The reporting period for the Assessments shall cover: (1) the first one hundred and eighty (180) days after service of the order for the initial Assessment, and (2) each two (2) year period thereafter for twenty (20) years after service of the order for the biennial Assessments. Each Assessment shall:



- A. set forth the specific privacy controls that Respondent has implemented and maintained during the reporting period;
- B. explain how such privacy controls are appropriate to Respondent's size and complexity, the nature and scope of Respondent's activities, and the sensitivity of the covered information;
- C. explain how the privacy controls that have been implemented meet or exceed the protections required by Part IV of this order; and
- D. certify that the privacy controls are operating with sufficient effectiveness to provide reasonable assurance to protect the privacy of covered information and that the controls have so operated throughout the reporting period.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Respondent shall provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by Respondent until the order is terminated and provided to the Associate Director of Enforcement within ten (10) days of request.

**Part VI. IT IS FURTHER ORDERED** that Respondent shall maintain and upon request make available to the Federal Trade Commission for inspection and copying, a print or electronic copy of:

- A. for a period of three (3) years from the date of preparation or dissemination, whichever is later, all widely disseminated statements by Respondent or its representatives that describe the extent to which Respondent maintains and protects the privacy, security, and confidentiality of any covered information, including, but not limited to, any statement related to a change in any website or service controlled by Respondent that relates to the privacy of such information, along with all materials relied upon in making such statements, and a copy of each materially different privacy setting made available to users;
- B. for a period of six (6) months from the date received, all consumer complaints directed at Respondent or forwarded to Respondent by a third party, that relate to the conduct prohibited by this order and any responses to such complaints;
- C. for a period of five (5) years from the date received, any documents, prepared by or on behalf of Respondent, that contradict, qualify, or call into question Respondent's compliance with this order;
- D. for a period of three (3) years from the date of preparation or dissemination, whichever is later, each materially different document relating to Respondent's attempt to obtain the consent of users referred to in Part II above, along with documents and information sufficient to show each user's consent; and documents sufficient to demonstrate, on an aggregate basis, the number of users for whom each such privacy setting was in effect at any time Respondent has attempted to obtain and/or been required to obtain such consent; and
- E. for a period of three (3) years after the date of preparation of each Assessment

required under Part V of this order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of Respondent, including but not limited to all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, for the compliance period covered by such Assessment.

**Part VII. IT IS FURTHER ORDERED** that Respondent shall deliver a copy of this order to (1) all current and future principals, officers, directors, and managers; (2) all current and future employees, agents, and representatives having supervisory responsibilities relating to the subject matter of this order, and (3) any business entity resulting from any change in structure set forth in Part VIII. Respondent shall deliver this order to such current personnel within thirty (30) days after service of this order, and to such future personnel within thirty (30) days after the person assumes such position or responsibilities. For any business entity resulting from any change in structure set forth in Part VIII, delivery shall be at least ten (10) days prior to the change in structure.

**Part VIII. IT IS FURTHER ORDERED** that Respondent shall notify the Commission within fourteen (14) days of any change in Respondent that may affect compliance obligations arising under this order, including, but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in either corporate name or address. Unless otherwise directed by a representative of the Commission, all notices required by this Part shall be sent by overnight courier (not the U.S. Postal Service) to the Associate Director of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line *In the Matter of FB, Inc.*, FTC File No.[ ]. *Provided, however*, that in lieu of overnight courier, notices may be sent by first-class mail, but only if an electronic version of any such notice is contemporaneously sent to the Commission at [Debrief@ftc.gov](mailto:Debrief@ftc.gov).

**Part IX. IT IS FURTHER ORDERED** that Respondent, within ninety (90) days after the date of service of this order, shall file with the Commission a true and accurate report, in writing, setting forth in detail the manner and form of their own compliance with this order. Within ten (10) days of receipt of written notice from a representative of the Commission, Respondent shall submit additional true and accurate written reports.

**V. REPRESENTATIVE FOREIGN AND DOMESTIC GOVERNMENTAL INVESTIGATIONS INTO FB'S USE AND ABUSE OF THE INFORMATION FB HAS COLLECTED FROM ITS USERS AND NON-USERS**

155. Plaintiffs repeat and re-allege all preceding and following paragraphs throughout

this Complaint as if fully set forth herein.

156. Upon receiving a number of complaints, the FTC investigated FB's privacy practices in 2011 which resulted in a consent decree barring FB from making any further deceptive privacy claims and required FB to obtain approval of the FB user' before it changed the way FB shared its user's information and required that FB undergo periodic assessments of its privacy practices by independent, third party auditors for 20 years.

157. In another of many admissions against interest and in response to the "Consent Decree" FB signed with the FTC in 2012, Zuckerberg stated, "I'm the first to admit that we've made a bunch of mistakes . . ."

158. On March 11, 2011, FB users sued FB for allowing advertisers on its platform unfettered access to the names, photographs, likenesses and identities of its users so that they could advertise all sorts of goods and services without the consent of their users. This lawsuit involved a FB feature called "Sponsored Stories," which essentially turned FB user's activity into an endorsed advertisement on their "Friends" pages, a feature of which FB's users were unable to opt-out of.

159. A \$20 million settlement was reached in this matter on May 10, 2012, in which FB agreed to revise its "Terms of Use" and parental controls, establish a settlement fund for authorized claimants to receive restitution and allocate additional funds to various charities. See FB, Inc., Docket No. C-4365 (FTC July 27, 2012) available at <https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810FBdo.pdf>. See also FB, *Analysis of Proposed Consent Order to Aid Public Comment*, FTC, Dec. 5, 2011

and Irina Ivanova, *FB's Past Failures*, *MSN Money*, Mar. 22, 2018 University of Cambridge Psychometrics Center. See also Complaint at *Fraley v. FB, Inc.*, Case No. 11-CV-196193, Cal. Super. Ct. Mar. 11, 2011.

160. On August 2011, FB user' Max Schrems, a German privacy rights lawyer, filed a Complaint against FB Ireland (FB's Irish subsidiary and the location of its European headquarters) with the Irish-based Office of the Data Protection Commissioner ("ODPC") concerning the access and use of FB user's information by developers of third party applications which constituted a tremendous threat to FB user' information. Schrems alleged that FB Ireland had no way "to ensure compliance with the limited contractual measures" it imposed on developers. While FB purportedly requires third party applications to have a privacy policy, not all third party applications have one. When a FB user connects to an application that does not have a privacy policy, FB hides the link to the privacy policy, instead of warning the FB user that there is no privacy policy.

161. As a result of Schrem's Complaint, the ODPC investigated and issued a "*Report of Re-Audit*" on September 21, 2012, which noted that FB Ireland had failed to adopt complete protection of FB user' information.

162. Specifically, the ODPC recommended to FB Ireland that: FB users must be informed to make a fully informed decision when granting unfettered access to third party applications; it must be made easier for FB users to understand that their activation and use of an application will be visible to their FB "Friends" as a default setting; it

should be made easier for FB users to make informed choices about what applications installed by “Friends” can access information about them. See *Amended Settlement Agreement and Release, Fraley v. FB, Inc.*, (Oct. 5, 2012) available at <https://www.scribd.com/document/120980082/Fraley-v-FB-Amended-Settlement-Agreement-2012-10-05>.

163. This compromise of FB user’ information also revealed that FB had been merging user’s information with information submitted by their contacts in order to create fuller profiles of its users. Essentially, information of non- FB users whose information may have been uploaded by “Friends” of FB users was being collected by FB and was also exposed to third parties.
164. On December 30, 2013, FB users filed a lawsuit against FB for scanning the content of their messages without consent for use in honing its advertisements in violation of the Electronic Communications Privacy Act and California’s Invasion of Privacy Act.
165. A non-monetary settlement agreement was reached in April 2017 in which FB enacted a number of changes to its ability to monitor and use its user’s communications for advertisement purposes as well as changes to its help center and overarching Data Policies. See FB Ireland Ltd., *Report of Re-Audit, Data Protection Commissioner*, Sept. 21, 2012. and Irina Ivanova, *FB’s past failures, MSN Money*, Mar. 22, 2018.
166. On September 11, 2017, the Spanish Agency for Data Protection (“AEPD”) announced that it had fined FB €1.2 million for violating information protection

regulations following its investigation to determine whether the processing carried out by FB complied with the information protection regulations.

167. The AEPD stated that its investigation verified that FB failed to inform users in a comprehensive and clear way about the information that it collects or about how such information is subsequently treated. In particular, the AEPD found that FB collects information derived from its user's communications with third party sites without informing them that FB collects such information or for what purposes it will later be used or disseminated.

168. The AEPD also found that FB's "Privacy Policy" contains generic and ambiguous language and requires clicking through a multitude of different links to view it in full. Further, the AEPD concluded that FB makes an inaccurate reference to the way it uses the information it collects, so even FB users with an average knowledge of new technologies would not become aware of FB's information collection, storage, aggregation or use policies.

169. In May 2017, the French information protection authority fined FB its maximum allowable fine of €150,000 for violations similar to those claimed by the Spanish authorities. The Commission *Nationale de 'Informatique et des Libertés* complained that FB "...proceeded to a massive compilation of personal user information of Internet users in order to display targeted advertising" and "it has also been noticed that FB collected information on the browsing activity of Internet users on third party websites without their knowledge." See Transcript of Zuckerberg's U.S. Senate hearing. See also the

*Washington Post*, Apr. 10, 2018 and Matthew Rosenberg, Nicholas Confessore, and Carole Cadwalladr, *How the Trump Consultants Exploited the FB Data of Millions*, *the New York Times*, Mar. 17, 2018; and Pariny Olson, *Face-To-Face with Cambridge Analytica's Elusive Alexander Nix*, *Forbes* magazine, Mar.20, 2018; and David Meyer, *Here's Why FB Got a \$1.4 Million Privacy Fine in Spain*, *Fortune*, September 11, 2017.

170. Six4Three the developer of a computer application called Pikinis, filed a lawsuit against FB, further undermining FB's repeated assertion that it has always prioritized its user's privacy. Pikinis was shut down approximately four years ago after FB blocked its third party unfettered access to a back-door channel to FB's user's "Friends" FB information.

171. In their lawsuit, Six4Three claimed that FB engaged in "an anti-competitive bait-and-switch scheme" that duped Six4Three, and thousands of other application developers into making hefty investments to build applications, only to later decide it would be in FB's best interest to no longer allow so many application developers unfettered access to its user's information and proceeded to block such access.

172. While FB has denied any wrongdoing in the Six4Three lawsuit, its blocking access action confirms that FB has always had the ability to change its access practices with respect to application developers, device manufacturers and others third parties accessing FB user's information, instead opting not to when it opted to aid and abet the Trump Campaign, Robert Mercer, Cambridge Analytica Russian operatives and others to sabotage the 2016 U.S presidential elections.

173. In 2014, even after FB changed certain of its third party access policies to FB's users' information, FB took a full year before ending third party application developer access, far more than enough time for application developers to plunder every FB user's information.
174. FB also failed to follow up on suspicious activity when security protocols were triggered, as noted by whistleblower Christopher Wylie. See Alex Hern and Jim Waterson, FB in public relations crisis mode over Cambridge Analytica scandal in the *Guardian*, Apr. 24, 2018.
175. FB's failure to detect and prevent the plunders of its user's information by Cambridge Analytica and other third parties or to adequately respond with proper notification and disclosures to FB users in accordance with best practices and applicable laws, belies any claim that FB's monitoring practices and internal information security and privacy policies were in any way sufficient.
176. Clearly, FB's user privacy protection policies, practices and procedures were willfully woefully inadequate because FB knew of the inadequacies since at least 2010 and did little of consequence to correct them.
177. FB violated the privacy of-hundreds-millions of American citizens, including Zimmerman's, and the negative impact of FB's failure to protect its user's privacy and FB's willful spread of Russian anti-American political propaganda for profit unless corrected is likely to continue far into the future and thus compound the suffering and damage FB has already inflicted on Plaintiffs and countless others.



178. A second FTC investigation of FB centers on whether FB violated a 2012 Consent Decree with that agency that required, among many other things, FB to receive explicit permission from users before it shared their personal information. FB gave broad unfettered access to its user's information to at least 60 companies with which it had information-sharing agreements.
179. Prosecutors from the U.S. attorney's office for the Eastern District of New York have been conducting a criminal investigation of FB, with a grand jury subpoenaing records from at least two smartphone manufacturers that had partnered with FB and who FB had allowed to access personal information from hundreds of millions of FB users.
180. The U.S. Department of Housing and Urban Development ("HUD") filed a civil complaint against FB, charging FB with discrimination in its advertising practices for housing. HUD is seeking damages for anyone harmed by FB's targeted advertising policies. A senior HUD official told CNBC it expects that millions of users may have been affected by the allegedly discriminatory policies based on the scale of FB's platform.
181. FB has since changed its advertising system to no longer allow employers and landlords to limit their targeted audience by race, ethnicity or gender and it recently settled a lawsuit over the practice.
182. The European Union's information protection watchdog group has launched multiple investigations into FB's privacy practices.
183. Ireland's Data Protection Commission released a report that disclosed fifteen ongoing investigations of major tech firms as of the end of 2018.

184. Of those investigations, 10 were focused on the way FB's user information is used by FB and included FB-owned Instagram and WhatsApp. The investigations largely centered around whether FB or its subsidiaries violated the European Union's General Data Protection Regulation ("GDPR").

185. FB was scheduled to appear in front of an appeals court in Brussels for a two-day hearing to challenge a 2018 court order, which said it must stop tracking users and non-users without their consent. In a press release published prior to the hearing, the Data Protection Authority said that it stands by the court's initial ruling and believes "that FB should be ordered to respect Belgian and European privacy rules when it processes personal information through its cookies, social plug-ins and pixels."

186. FB has appealed a ruling from Germany's Federal Cartel Office that called into question FB's business model and said it "overstepped" the boundaries of GDPR, especially in light of what it called "FB's dominant position" in the market. "There is no effective consent to the [FB] user's information being collected if their consent is a prerequisite for using the FB.com service in the first place," the case summary stated.

187. FB defied a summons and did not attend a hearing at the Canadian Parliament. Lawmakers from 10 countries, including the U.K. and Australia, are scheduled to attend the meeting. "Collectively we represent about 450 million people, it's a bigger population group than the U.S.," Bob Zimmer, the chairman of the Canadian parliamentary committee hosting the international meeting, told CNN.

188. Zimmer said he wanted to hear from FB's top two executives [Zuckerberg and Sandberg] who had opted out, not their replacements. "Knowing the structure of FB and how it is micro-managed right from the top, any change on the platform is done through Mr. Zuckerberg or through Ms. Sandberg."

189. "It's not that hard to jump on a plane and make some time to hear from legislators and answer their questions," Zimmer told CNN. Zimmer added that the decision to hold the two in contempt would be voted on by the whole of Parliament. "Nobody is going to come with some handcuffs and arrest them, but to be held in contempt by an entire country would not serve any platform well," he added.

**VI. FB' CONSPIRATORIAL CONDUCT AND ADMISSIONS REGARDING THEIR ROLE IN THE SABOTAGE OF THE 2016 U.S. PRESIDENTIAL ELECTION CYCLE**

190. Plaintiffs repeat and re-allege all preceding and following paragraphs as if fully set forth herein.

191. Zuckerberg has admitted over and over again that FB user's information was repeatedly plundered by third parties and others.

192. But these admissions came only after the FB user' information plunders and other FB election compromises were reported in the media and led to the public outrage that induced several congressional inquiries into FB's involvement in the sabotage of the 2016 U.S. presidential elections and other unlawful conduct.

193. Zuckerberg paved the way for the sabotage of the 2016 U.S. presidential elections when on October 1, 2012 Z he met with Russian Prime Minister Dmitry Medvedev in Moscow and can be seen in a photo with the Russian Prime Minister glad-handing and smiling profusely as he hands Medvedev a T-shirt inscribed on the front [www.FB.com/DmitryMedvedev](http://www.FB.com/DmitryMedvedev). It's possible Zuckerberg was compromised before he dropped out of college or shortly thereafter.
194. Zuckerberg who willingly travelled to Moscow, declined to travel to England to answer charges being contemplated against FB being brought by the British government. Surely the Medvedev meeting involved more than a T-shirt.
195. Zuckerberg willfully lied over and over again when he publicly declared that "The security of [FB users] privacy allows FB users to freely engage and share their feel free to connect because they know that their privacy is going to be protected." See, <https://www.cnn.com/2018/04/03/zuckerberg-on-FB-and-privacy-before-cambridge-analytica-scandal.html>.
196. However, long before and contrary to Zuckerberg's self-serving public pronouncements regarding FB user' contentedness with FB user' information privacy protections, FB launched a multifaceted strategy that willfully, recklessly and dangerously violated its user's right to privacy.
197. Never before has any U.S. company exploited its customer's stored information for profit and market power or actively engaged in the cyber-sabotage of U.S. elections as did FB. See *Trump Consultants Exploited the FB Information of Millions*, *New York Times*

(Mar. 17, 2018) See also, Carole Cadwalladr, *'I Made Steve Bannon's Psychological Warfare Tool': Meet the Information War Whistleblower*, the *Guardian* (Mar. 18, 2018).

198. In the wake of the media's public disclosure of FB's willful FB user privacy protection deceptions, Zuckerberg admitted: "[I]t's clear now that we didn't do enough. We didn't focus enough on preventing abuse and thinking through how people could use these tools to do harm as well. That goes for fake news, foreign interference in elections, hate speech, in addition to developers and information privacy. We didn't take a broad enough view of what our responsibility is, and that was a huge mistake. It was my mistake."

199. Zuckerberg's admission that FB's role in the sabotage of the 2016 U.S. presidential elections was "my mistake" is an outrageous euphemism.

200. There was no mere Zuckerberg "mistake."

201. Instead and conversely, FB aggressively sought the advertising dollars of anti-democratic advertisers and hate mongers, including those of Russian operatives, the Trump Campaign, Robert Mercer and numerous others and they were well aware that its FB user's information was not only plunderable but also, at their direction and consent, had been made widely available by FB to an assortment of third parties, certain of which sought to undermine America's democratic institutions, free and fair elections, constitutional protections, free and fair markets and much, much more.

202. Before, during and after the President assumed the Office of the Presidency, the Trump Campaign conspired with and paid FB millions of dollars to spread lies, disinformation and misinformation to influence FB users and others to vote for Trump, to

promote white supremacy, to coverup Russia's role in the sabotage of the 2016 U.S. presidential elections, to divide America's electorate, to disparage Trump's political opponents, to denounce the judiciary and humiliate persons opposed to the Trump candidacy and to demean and cheapen the institutional pillars of America's democracy.

203. While Zuckerberg has commented that FB was as surprised as anyone by the mammoth 2014 FB user' information plunder, in fact FB actually encouraged the plundering by allowing numerous third parties unfettered access to its user information repositories and its willfully lax approach to protecting the privacy of its user's information.

204. A 2011 FTC Complaint specifically references FB allowing third party unfettered access to FB user' information and convinced FB to sign a multi-count "Consent Decree" to correct its deceptive privacy protection , which FB has, for the most part, willfully and recklessly ignored.

205. During his testimony before the Senate Commerce and Judiciary Committees on April 10, 2018 and testimony before the House Energy and Commerce Committee on April 11, 2018, Zuckerberg admitted that "[FB] didn't take a broad enough view of [its] responsibility [on information privacy] stating: "It was my mistake. And I'm sorry. I started FB, I run it, and I'm responsible for what happens here."

206. Zuckerberg committed to improve his company's security, including the basic responsibility of protecting the privacy of FB user' information, which he entirely and willfully failed to do.

207. In 2018, Senator Amy Klobuchar (D-Minn.) made it clear to Zuckerberg that Congress disapproves of FB's current privacy efforts. She stated: "I think we all agree that what happened here was bad. You acknowledged it was a breach of trust. And the way I explain it to my constituents is that if someone breaks into my apartment with the crowbar and they take my stuff, it's just like if the manager gave them the keys or if they didn't have any locks on the doors, it's still a breach; it's still a break in." Todd Shields and Vonnie Quinn, *FB Could Be Fined Millions for Violating Consent Deal*, *Bloomberg News*. Mar. 29, 2018.

208. Similarly, Senator Catherine Cortez Masto questioned Zuckerberg on FB's privacy policies and on whether FB had violated the 2012 FTC "Consent Decree."

209. There are eight counts of deceptive acts and practices in the November 2012 FTC "Consent Decree" that bar FB from, among other things, any further deceptive privacy claims.

210. And, most importantly, the FTC "Consent Decree" required FB to give its users clear and conspicuous notice and to obtain affirmative express consent before sharing their information with third parties.

211. Senator Cortez asked Zuckerberg, "That was part of the FTC "Consent Decree," correct?"

212. Zuckerberg answered: " Senator, that sounds right to me."

213. Continuing through his testimony before the U.S. Senate, Zuckerberg also admitted that FB made a mistake in not following up with Cambridge Analytica in 2015 to ensure the FB user' information they plundered from FB was, in fact, deleted.
214. Zuckerberg also stated that he "clearly viewed it as a mistake that we didn't inform people" about the misappropriation of their information at that time, and also did not notify the FTC in 2015, despite the 2012 "Consent Decree" to do so.
215. Despite FB's lengthy and oft repeated privacy protection promises and a still active FTC 2012 "Consent Decree" setting forth a number of FB information security obligations, FB failed to prevent the aggregation of the information of millions of its users, thereby exposing those users to potential unauthorized use of their information in the future. See FTC press release, "*Statement by the Acting Director of FTC's Bureau of Consumer Protection Regarding Reported Concerns about FB Privacy Practices*", Mar. 26, 2018 and transcript of Zuckerberg's U.S. Senate hearing, the *Washington Post*, Apr. 10, 2018.
216. Making the malfeasances of FB even worse, in the days after the 2016 U.S. presidential elections, Zuckerberg dismissed as "crazy" any suggestion that disinformation, misinformation, fake political propaganda and more broadcast by Russian intelligence agents and operatives, the Trump Campaign Robert Mercer and others on FB could have swayed the elections, a position the President maintains still.
217. Zuckerberg has since said he regrets making that and other comments, yet FB has done little to fix its lax privacy protection measures to preclude the use of FB user' information to unlawfully sway future elections, though it did block the political messages





of Senator Elizabeth Warren and continues to block Zimmerman from promoting his books on FB, books that express political ideas very similar to those of Senator Warren's and to use FB for any purpose whatsoever.

218. Meanwhile Zimmerman's FB "Friends" continue to communicate with him using FB, but he is blocked from communicating with them.

219. FB is willfully engaged in censoring political speech on a highly selective basis, lawful and non-violent political speech that is historically given the highest protection under the First Amendment to the U.S. Constitution and numerous state constitutions, including those of California and North Carolina is censored by FB, while that of Russian operatives and terrorists is not.

220. In a self-serving but ineffectual effort to gain sympathy, while testifying before Congress Zuckerberg said even his own FB user' information was plundered.

221. Prior to his congressional testimony, Zuckerberg set up a war room at FB headquarters and spent months preparing his congressional testimony, actions hardly necessary if he was going to testify truthfully.

222. Not once has FB disclosed to Plaintiffs or possibly any other FB user just how often and by whom Plaintiff's FB user' information and that of their FB "Friends" was accessed and/or collected and used by third parties, or how, if at all, FB would prevent and/or remedy future domestic and foreign compromises and the further spread of already compromised information of their FB user' information.

223. What was disclosed are photos of Zuckerberg in Moscow on October 1, 2012 glad-handing and smiling profusely as he hands Russian Prime Minister Dmitry Medvedev a T-shirt.
224. Like many another huge organization that has faced the prospect of congressional and regulatory agency investigations into its alleged unlawful activity, FB hired dozens of expensive attorneys and lobbyists to arrange to dilute and/or thwart those congressional and regulatory investigations. D.C. floats on a deep pool of cash, a commodity FB has plenty of.
225. In an admission against interests, FB stated that those who plundered the information of FB users would not face consequences from FB.
226. The chairman of the *New York Times* referred to Zuckerberg's views regarding the news of FB's plundered user' information as "a terrifyingly naïve perspective that makes my blood run cold and the CEO of *NewsCorp* said "We have entered into an era where the pervasiveness of FB makes Standard Oil look like a corner gas station" and the editor-in-chief of *Wired* magazine said: "News publishers have been reduced to sharecroppers on FB's massive industrial farm."
227. Congressman David Cicilline stated: "No question that we have reached a tipping point; we stand at the precipice of sacrificing the news organizations that are central to uncovering corruption, holding the government and giant corporations accountable."
228. Zuckerberg has admitted that it was his and FB's actions and inactions that helped allow the tens-of-millions of FB user's Cambridge Analytica plundered information from

to rig the 2016 U.S. presidential elections against Secretary Clinton and in favor of the President, actions and inaction coordinated with the Trump Campaign, Russian intelligence agents and operatives, Robert Mercer and others, a form of cyberwarfare that is possibly treasonous.

229. A New York State Attorney General joined with his Massachusetts counterpart in her investigation into FB's handling of FB user' information stating that: "Consumers have a right to know how their information is used and companies like FB have a fundamental duty to protect their user's information."

230. There are all sorts of privacy protection obligations that FB promised to undertake and then failed to undertake under the terms of the FTC 2012 "Consent Decree" and FB faces heavy monetary fines and other penalties after a second (2018) FTC's investigation found that FB failed to address the numerous charges of misconduct set out the 2012 FTC "Consent Decree" that FB agreed to remedy.,

231. In August 2019, the FTC fined FB \$ 5 billion for its misconduct, less than one month's revenues and testament to the influence of the expensive attorneys and lobbyists FB hired to defend it against the FTC's charges.

232. FB has been aware of the misappropriation and misuse of FB user' information since at least 2010 and yet has done little to protect that information or notify FB users whose information was sold or traded by FB or plundered by third parties, deceptive, willful and reckless FB action and inaction that constitutes numerous violations of state and federal laws dealing with compromised information.

233. Plaintiffs and countless other FB users trusted FB because FB's tedious, non-negotiable contract states: "You own all of the "... information you post on FB, and you can control how it is shared through your privacy and application settings." This and other FB promises are willfully , intentionally deceptive, false and misleading. Quote, as above, taken from FB "Terms of Service," dated January 30, 2015. <https://www.FB.com/terms>.

234. FB's "Terms of Service" includes hundreds of intentionally incomprehensible pages that are universally unread or misunderstood by FB users.

235. Moreover, also without user consent, FB has repeatedly modified the "Terms of Service" and other sections of its contract with its users to suit only its own purposes.

236. Between 2011 and 2012, Sandy Parakilas was the FB platform operations manager responsible for policing the use of FB user' information by third party application developers and others.

237. IN 2011, Parakilas provided FB senior executives with a detailed presentation outlining FB's user information vulnerabilities. Certain of his warnings follow: "My concerns were that all of the information that left FB servers to developers could not be monitored by FB, so we had no idea what developers were doing with the information," Parakilas maintained, adding that "FB had "Terms of Service" and settings that people didn't read or understand and FB did not use its enforcement mechanisms, including audits of external developers, to ensure information was not being misused."

238. FB Defendants did nothing to address the Parakilas security warnings. See <https://www.washingtonpost.com/opinions/i-worked-at-FB-i-know-how-cambridge->

analytica-could-have-happened/2018/03/20/edc7ef8a-2bc4-11e88ad6FBc50284fce8\_story.html?utm\_term=.faaca3c6d7b4.

239. “It has been painful watching,” Parakilas said, “...because I know that FB could have prevented it.”

240. FB’s failure to adequately protect its FB user’ information is further documented at <https://www.theguardian.com/news/2018/mar/20/FB-information-cambridge-analytica-sandy-parakilas>.

241. To repeat, FB’s non-negotiable contract with its users’ states: “You own all of the information you post on FB, and you can control how it is shared through your privacy and application settings.”

242. Yet, FB intentionally breached this and other contractual provisions as alleged herein. Thus, FB willfully, deceptively, recklessly and dangerously misled its users into believing that FB would protect the privacy of their FB user’ information.

243. Explicit FB policy further prohibits “any action...that infringes or violates someone else’s rights or otherwise violates the law.” However, as Parakilas later revealed, FB did enforce its user information privacy protection policy.

244. By way of illustration, Parakilas described an infringement by a computer application called Klout, which was creating unauthorized profiles of children.

245. Parakilas was tasked by FB with calling a Klout executive to ask whether it was violating any FB policies because FB had no other way of verifying violations.



246. The Klout executive assured Parakilas it was not violating any FB policies and FB took no further action with regard to the Klout violations.
247. In December 2015, the *Guardian* published an article that exposed the unauthorized plunders of nearly a hundred million FB users by Cambridge Analytica on behalf of Senator Ted Cruz's 2016 presidential campaign. See <https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president.->
248. The Cambridge Analytica plunders of FB user' information was funded and directed by Robert Mercer (a megadonor and informal advisor to the Trump Campaign) and Steve Bannon (a former Trump Campaign and Trump administration senior political strategist and advisor) to sabotage the 2016 U.S. election cycle.
249. For reasons as yet unknown, Bannon is cited over 100 times in the Special Counsel's redacted report, while Robert Mercer and his partner in unlawful political conduct Rebecka Mercer are not so cited.
250. Upon reviewing FB's request to delete the FB illicitly obtained user information, Cambridge Analytica' whistleblower Christopher Wylie said he was "...astonished by FB's lackluster response...All they asked me to do was tick a box on a form and post it back." See <https://www.theguardian.com/news/2018/mar/17/information-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump>.
251. On June 18, 2016, FB executive Andrew Bosworth defended FB's aggressive growth tactics, stating in a memo entitled *The Ugly* obtained by *BuzzFeed* that highlighted many of FB's questionable practices and elevated FB's quest for infinite growth above all



else, even the security, privacy and safety of its users by stating: “We connect more people. That can be bad if they make it negative. Maybe it costs a life by exposing someone to bullies. Maybe someone dies in a terrorist attack coordinated on our tools. And we still connect people. the ugly truth is that we believe in connecting people so deeply that anything that allows us to connect more people more often is de facto good. It is perhaps the only area where the metrics do tell the true story as far as we are concerned.” See <https://newsroom.FB.com/news/2018/03/suspending-cambridge-analytica/>.

252. Given the cult of growth at any cost instigated by FB Defendants and as documented in Bosworth’s memo, FB’s proposed remedial measures are grossly inadequate as corrective measures to assure the protection of FB user’ information and were announced only after Cambridge Analytica’s plunder of nearly a hundred million FB user’s information made headlines and Congress and law enforcers began investigating FB’s user’ information protection failures.

253. FB Defendants deceptive, willful and reckless actions and inactions caused Plaintiffs to suffer, among other things, the following harms:

- (1) Plaintiffs have zero control over their information or how that information is used by FB and third parties.
- (2) The value of Plaintiff ‘s FB user information has been diminished because it is no longer private and is readily available to third parties throughout the world.
- (3) Plaintiff’s FB user’ information has been abused and misused by FB and is still vulnerable to future abuse and misuse.

- (4) There is no way Zimmerman can secure his FB user information or protect it from future misuse and abuse because, among other reasons, FB has blocked Zimmerman from accessing his information and his FB accounts and Zimmerman has not the means to learn who has his FB user' information or how it has been or will be used.
- (5) Zimmerman has had his opportunity to participate in the political process diluted by virtue of being improperly targeted with illegal propagandistic political messages in the past and in the foreseeable future.
- (6) Zimmerman has lost his opportunity to use the FB platform to support the candidates of his choice among his FB user' "Friends" and others.
- (7) Zimmerman was unable follow his plan to market his books using FB because his accounts were blocked by FB.
- (8) Zimmerman suffered and is still suffering monetary losses and significant emotional distress from the sabotage of the 2016 U.S. presidential elections as willfully and recklessly aided and abetted by FB.
- (9) FB users and Zimmerman's FB user' "Friends" continue to communicate with him but since Zimmerman's FB accounts remain blocked, Zimmerman cannot communicate with them.

254. Zimmerman, like many other FB users, had thousands of FB "Friends" and intended to use the FB platform to support certain political candidates and as his primary means to market his pro-democracy political books and his novel.

255. FB's willful and reckless failure to adequately prevent the illegal course of conduct herein alleged regarding the plunder of FB user' information, including Plaintiff's, leaves that information dangerously unprotected and open to further improper and illegal use and abuse, such as identity theft and elections manipulation.
256. The access to FB user' information granted by FB to third parties and plundered from FB is extremely valuable. The names, email addresses, recovery email accounts, telephone numbers, birthdates, passwords, security question answers, and other information can all be used to gain unfettered access to a variety of Plaintiff's online commercial, informational and other resources.
257. Identity thieves use plundered information to harm their victims through embarrassment, blackmail, or harassment in person or online, or to commit other types of fraud including obtaining ID cards or driver's licenses, fraudulently obtaining tax returns and refunds, and obtaining government benefits.
258. A presidential report on identity theft from 2008 states that: "In addition to the losses that result when identity thieves fraudulently open accounts or misuse existing accounts,...individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration."

259. In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can amount to a considerable amount of time and money to repair the damage caused by the identity thieves.

260. For example, victims of identity theft must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors. See, the President's Identity Theft Task Force, Combating Identity Theft: A Strategic Plan, Federal Trade Commission, 11 (April 2007), <http://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theft-strategic-plan/strategicplan.pdf>.

261. The problems associated with identity theft are exacerbated by the fact that many identity thieves will wait years before attempting to use the information they have obtained. Indeed, Zimmerman will need to remain vigilant against unauthorized information use for the rest of the limited time he has left.

262. Once plundered, FB user' information can be used in a number of different ways, including sale on the "Dark Web," a heavily encrypted part of the Internet that makes it difficult for authorities to detect the location or owners of a website.

263. The "Dark Web" is not indexed by Google and is only accessible using a Tor browser (or similar tool), which aims to conceal user's identities and online activity. The

“Dark Web” is notorious for hosting marketplaces selling illegal items such as weapons, drugs, and plundered information.

264. Once someone buys plundered victim information, it is then used to gain unfettered access to different areas of the victim’s digital life, including bank accounts, Internet-based platforms and credit card details. During that process, other sensitive information may be harvested from the victim’s accounts, as well as from those belonging to family, friends, and colleagues.
265. In addition to the information it contains, a plundered FB account can be very valuable to cyber criminals.
266. Since FB accounts are linked to myriad financial and non-financial accounts, a plundered FB user’ account offers plunderers countless opportunities to ply their illegal and harmful pursuits. See, Brian Hamrick, *The Dark Web: A trip into the Underbelly of the Internet*, *WLWT News* (Feb. 9, 2017 8:51 PM), <http://www.wlwt.com/article/the-dark-web-a-trip-into-the-underbelly-of-the-Internet/8698419>.
267. Adding to Plaintiff’s fear that their information has been plundered by identity thieves is the fact that none of FB’s alleged remedial actions included giving proper notice to Plaintiffs that their FB user’ information may have been plundered.
268. Plaintiffs had been registered FB users with thousands of FB “Friends” for several years before FB blocked their accounts and had provided FB their information as consideration for the use of the FB platform and relied on FB’s contractual promises to protect their information from access and use by third parties.

269. Plaintiffs have never consented to allowing FB or any third party to sell, trade or allow unfettered access to their FB user' information for political or any other purpose.

270. Plaintiffs believe they are among the millions of Americans whose FB user' information was plundered by Cambridge Analytica.

271. Zimmerman has no way to learn how many information plunderers and non-plunderers have had unfettered access to and collected for future use Plaintiff's FB user information.

272. Zimmerman could not have been reasonably expected to know that FB's stored user' information could be plundered, aggregated, targeted and then used for improper and illegal purposes, including the sabotage of the 2016 U.S. presidential elections.

273. The *Economist* magazine reported in 2017 that: "The world's most valuable resource is no longer oil, but information."

274. FB captured and stored information includes: person and company names and addresses, hometowns; birthdates; gender; family connections; educational achievements; email addresses; relationship statuses; work histories; personal and business interests; hobbies, religious and political affiliations; phone numbers; dates and times of active sessions on FB; dates and times and titles of advertisements ; connections with other FB users and non-users; communications with other FB users, current and last locations; attendance at events and social gatherings, stored credit card information, the people the FB user' is "Friends" with and/or follows, FB groups the FB user' is a member of; a list of Internet addresses where FB users have used while using their FB accounts, posts or

sites the FB user' has liked, searches conducted by the FB user, photographs and videos documenting all aspects of a FB user's life and the lives of his "Friends" and family; and their activity in FB-connected applications.

275. FB's information storage repositories contain multiple quintillions of FB user' and non-user' information as amassed from billions of persons and businesses throughout the world. One quintillion of information is the equivalent of all of the words ever uttered since Adam and Eve first spoke in the "Garden of Eden."

276. FB Defendants have schemed to monetize in various ways its vast store of FB user' and non-user information in conscious disregard for the contractual and constitutional rights of its users and non-users and by so doing have inflicted enormous damage on them and on Plaintiffs.

277. FB has successfully willfully misrepresented itself as an eleemosynary enterprise that enables free communication among its users, when, in fact, it was selling and trading strategically targeted unfettered access to FB stored user' information to commercial and political advertisers such as the Russian operatives and intelligence agents thirteen of which remain indicted by the Special Counsel and fugitives from justice..

278. FB's practice of selling targeted unfettered access to FB user' information was an willful FB business strategy designed and implemented by FB to increase FB revenues and market power by monetizing its user's information, a business strategy that proved wildly successful and created huge incentives for FB to ignore the 2012 FTC "Consent Decree" it had signed.

279. Additionally, FB collects user' information from Instagram, Messenger and Whatsapp, three other media/mobile applications that FB owns and manages, making it impossible to assess how much FB user' information has been sold or traded by FB and plundered by third parties with and without FB's knowledge and/or permission.
280. FB executives have admitted that third parties have used FB's "Friend" search function to plunder FB user' information by submitting phone numbers or email addresses they already have through FB's search and account recovery, stating: "Given the scale and sophistication of malevolent third party activity, we believe 'most people' on FB could have had their public profile scraped in this way."
281. "Most people" on FB means that we're talking about at least hundreds-of-millions of FB users whose FB user' information has been spirited away into countless third party information repositories.
282. A vital feature in the rapid growth in the numbers of FB users is the false sense of control FB users, including Plaintiffs, have been led by FB to believe they have over their information.
283. FB's privacy settings purport to offer FB users control over the dissemination of various categories of their user' information, whether it be privately with particular FB users, or with all of their FB user' "Friends", or with "Friends" of FB "Friends", or with all FB users. See <https://www.cnbc.com/2018/04/04/FB-updates-its-terms-of-service-to-include-messenger-instagram.html>.



284. Thus, FB users reasonably expected that their information would only be accessible to the extent they authorized such access. See <https://www.theatlantic.com/technology/archive/2018/04/most-people-on-FB-may-have-had-their-accounts-scraped/557285/>.
285. In reality, the information of FB users was not within the control of FB users, but instead had been plundered by Cambridge Analytica (a foreign business entity funded and directed by U.S. citizen Robert Mercer) and was used by FB, Russian intelligence agents and operatives, the Trump Campaign, Robert Mercer and others who conspired to and succeeded in sabotaging the 2016 U.S. presidential elections.
286. FB's greed and quest for ever increasing profit and monopolistic market power enabled third parties like Cambridge Analytica to unlawfully appropriate the FB user information of nearly a 100 million FB users, information that was later used by FB, Russian intelligence agents and operatives, the Trump Campaign, Robert Mercer and others to successfully sabotage the 2016 U.S. presidential elections.
287. Beyond those FB' efforts to undermine the fundamental constitutional right of Zimmerman to vote in a free and fair elections, FB, Russian intelligence agents and operatives, the Trump Campaign, Robert Mercer and others sought to and did destabilized U.S. democratic institutions and the rule of law.
288. Zuckerberg has publicly admitted more than once that people share information on FB because "...they know their privacy is going to be protected. the security of privacy allows FB users to freely engage and share their feel free to connect because

they know that their privacy is going to be protected.” See <https://www.cnbc.com/2018/04/03/zuckerberg-on-FB-and-privacy-before-cambridge-analytica-scandal.html>.

289. In the weeks leading up to the 2016 U.S. presidential election cycle, Roger McNamee, one of FB’s most influential investors, sounded the alarm about the FB user’ information being accessed by and used by numerous authorized and unauthorized third parties.
290. FB ignored McNamee’s concerns and it was not until other brave whistleblowers came forward that FB finally acknowledged the Cambridge Analytica plunders of FB user’ information.
291. Willfully ignoring the 2012 “Consent Decree” it had signed with the FTC, FB did not provide any notice to its users, including Plaintiffs, of the user’ information breaches, making injunctive relief particularly urgent.
292. FB has not only failed to provide any notice of the FB user’ information breaches to its FB users, but instead has, until recently, much like the President’s oft repeated denial that there were Russian intrusions in the 2016 U.S. presidential election cycle, steadfastly denied there were breaches of its users’ information.
293. The FB user’ information breaches are far more egregious than the notorious Equifax information breach because Equifax disseminated notice to its customers of the information breach and provided a way to verify whether a particular consumer’s information was plundered.

294. Instead, FB willfully suppressed information about the information breaches until investigative reporters brought it to public attention, and even then FB did nothing much to further inform its users that their information had been plundered or what FB or FB users could do to protect themselves or how their plundered information could be used to damage them. See <https://economictimes.indiatimes.com/tech/Internet/information-breach-claims-false-FB/articleshow/63353256.cms>.

295. This action seeks to hold FB accountable for, among other things, their roles in facilitating the sabotage of the 2016 U.S. presidential elections, for blocking Plaintiff's FB accounts while allowing unfettered access to now indicted Russian intelligence agents and operatives, the Trump Campaign, Cambridge Analytica, Robert Mercer and numerous unnamed others to use FB to successfully sabotage the 2016 U.S. presidential election cycle, for subjecting Plaintiffs to future identity theft and other nefarious activities and for falsely inducing Plaintiffs to use the FB platform by contractually promising to protect Plaintiff's FB user information.

296. FB obtains the lion's share of its revenue from advertisers.

297. FB's 2017 corporate financial statement lists one of the major risks to its business as a "...decrease in user engagement, including time spent on our products."

298. Another FB-stated major risk to FB's business is the potential decline in "the effectiveness of our strategic ad targeting and the degree to which users opt out of certain types of ad targeting, including as a result of changes that enhance the user's privacy."

299. With regard to FB's strategic ad targeting, FB is now legally bound to stop advertisers from discriminating against people because of their race and other factors.

300. FB is now legally bound to never again allow those advertising on FB to discriminate against Americans on the basis of race, national origin, religion, sexual orientation and other protected categories, a widespread FB advertiser practice that the State of Washington deemed "unlawful discrimination."

301. The FB settlement with Washington State resulted from a two-year probe. Because it is legally enforceable, the settlement holds FB to a higher standard than previous commitments, which previously had been voluntary and ignored by FB. It also expands the types of ads that will receive more enforcement from FB to include insurance and "public accommodations", two categories FB had never explicitly said were covered under its anti-discrimination efforts.

302. The Washington State probe stemmed from reports in *ProPublica*, beginning in 2016, that found advertisers, using FB's strategic micro-targeting tools, could conceal housing ads from African American users and other minorities. Investigators in the Attorney General's office said that they tested the system by creating "20 fake ads" on FB as part of their investigation in November and December 2017, touching everything from nightclubs to employment opportunities, that "excluded one or more ethnic minorities."

303. After *ProPublica's* investigation, FB said it would no longer let advertisers strategically target ads for housing, credit offers and employment by "ethnic affinities," a

category that the social network had created to enable businesses to reach minority groups.

304. Even after the FB's voluntary pledge, reports revealed that FB advertisers who posted housing ads were still able to exclude people on the basis of race, calling into question FB's promise of stepped-up enforcement. FB's ad system also automatically approved housing ads that excluded mothers of high school kids, Jewish people and Spanish speakers.

305. As a presidential candidate and then as President, Trump has lied to the American people well over 10,000 times, including repeated denials of the Russian government's participation in the sabotage of the 2016 U.S. presidential elections, contravening the U.S. National Security Intelligence Community and the Special Counsel's report that has made it clear that Russian covert operations made use of FB and other Internet-based platforms in a successful effort to sabotage the 2016 U.S. presidential elections.

306. Russian trolls amassed hundreds of thousands, possibly millions, of American followers on FB, targeted them during the 2016 U.S. presidential elections with a multi-faceted campaign of anti-democratic political propaganda and pro-Trump anti-Clinton advertisement, paid for in part with Russian rubles, while FB sat back observing the online sabotage, profiting from it and actively participating in the sabotage by assigning FB employees to the Trump Campaign's San Antonio 100-person information processing facility, where the Cambridge Analytica-created voter profiles of millions of American FB users were used to help in the sabotage the 2016 U.S. presidential elections.

307. Plaintiff Zimmerman is an American citizen and veteran who voted in the 2016 U.S. presidential elections (primary and general) with the reasonable expectation that the elections would be free and fair and not sabotaged by FB, Russian intelligence agents and operatives, the Trump Campaign, Robert Mercer, Cambridge Analytica and others, and that the privacy of his FB user' information and that of his FB "Friends" would be protected by FB and not used to help sabotage the 2016 U.S. presidential elections.

308. President Abraham Lincoln once said: "I see in the near future a crisis approaching that unnerves me and causes me to tremble for the safety of my country...corporations have been enthroned, an era of corruption in high places will follow, and the money-power of the country will endeavor to prolong its reign by working up the prejudices of the people until the wealth is aggregated in a few hands and the republic is destroyed."

309. These omniscient thoughts of President Lincoln are borrowed from a book of poetry entitled *Patriotic Poems of Freedom*, written by Natasha H. in 2001, when she was ten years old.

310. Corrupt foreign and domestic business entities, billionaires, political organizations and individuals such as Robert Mercer, Mark Zuckerberg, Sheryl Sandberg, the Trump Campaign and the Trump Organization and their numerous unnamed co-conspirators, including Russian President Putin, Russian, Ukrainian and Balkan oligarchs and their numerous agents and operatives are metastasizing, malignant cancers eating away at the pillars of our democratic institutions.

311. Bending toward transparent justice, our democracy does so by force of law as guided by our judiciary and supported by the grassroots efforts of “We the People.”

312. Every now and then Americans are confronted by pure evil in the form of terrorists like Hitler, Stalin, bin-Laden and now a new form of evil, cyber-terrorists.

313. During the last week of August 2017, U.S. Secretary of Defense James “Mad Dog” Mattis and U.S. Secretary of State Rex Tillerson condemned the President’s anti-democratic values and actions, stating in effect that the President speaks for himself and not for them, and not necessarily in America’s best interests, stopping just short of calling the President’s words and actions those of a home-grown terrorist.

314. The President countered calling his self-appointed Secretary of State Rex Tillerson “dumb as a rock.”

315. General Mattis, described the President’s understating of the world as that of "a fifth or sixth grader."

316. At a White House meeting, the President’s former Chief of Staff, four-star General John Kelly, said of the President: "He's an idiot. It's pointless to try to convince him of anything. He's gone off the rails, we're in Crazytown. I don't even know why any of us are here. This is the worst job I've ever had.

317. And the President's former personal lawyer John Dowd described the President as "a fucking liar," telling the President he would end up in an "orange jump suit" if he gave oral testimony to the Special Counsel’s investigation into Russian interference in the 2016 U.S. presidential elections.

318. In one numerous obstructions of justice, the President refused to give oral testimony to the Special Counsel and declined to answer a preponderance of written question proffered by the Special Counsel.
319. In addition to influencing our elections, invading our privacy, censoring our free speech, actively working to defile our democratic institutions and ruining competitors with its monopolistic practices and efforts to control consumer behavior, now FB wants to introduce its own currency.
320. Following U.S. banking giant J.P Morgan Chase's launch of cryptocurrency JPMCoin, FB is planning to launch its own cryptocurrency in early 2020, allowing its users to make digital payments in dozens of countries.
321. In 2018, FB asked U.S. banks to share detailed financial information about their customers.
322. The FB created cryptocurrency, named GlobalCoin, would enable FB's billions of users to change dollars and other international currencies into its digital coins. The coins could then be used to buy things on the Internet and in shops and other outlets, or to transfer money without needing a bank account.
323. According to the BBC, Zuckerberg met the governor of the Bank of England, Mark Carney, to discuss its cryptocurrency plans.
324. Zuckerberg has also discussed the cryptocurrency proposal, known as Project Libra, with U.S. Treasury officials and is in talks with money transfer firms, including Western Union.



325. Zuckerberg told the FB's developer conference: "I believe it should be as easy to send money to someone as it is to send a photo."

326. In order to try to stabilize the digital currency the company is looking to peg its value to a basket of established currencies, including the U.S. dollar, the euro and the Japanese yen.

327. FB is also looking at paying its users fractions of a coin for activities such as viewing FB ads and interacting with FB content related to online shopping.

328. However, experts believe that regulatory issues and FB's poor track record on data privacy and protection are likely to prove to be the biggest hurdles to making FB's cryptocurrency a success.

329. "FB is not regulated in the same way as banks are, and the cryptocurrency industry is, [for the most part,] unregulated," said Rebecca Harding, chief executive of banking trade data analytics firm Coriolis Technologies.

330. The U.S. Senate Banking Committee wrote an open letter to Zuckerberg asking how the currency would work, what consumer protection would be offered and how information would be secured.

331. It emerged recently that FB is looking for funding to support the project and has held talks with payments giants including Visa and Mastercard.

332. FB has been long expected to make a move in financial services, having hired the former PayPal president David Marcus to run its messaging application in 2014.

333. Marcus, a board member of crypto exchange Coinbase, runs FB's blockchain initiatives, the technology on which cryptocurrencies run.
334. FB's staff has already had unfettered access to hundreds of millions of FB user' passwords and used them for nefarious purposes.
335. FB has admitted that it has not properly masked the passwords of hundreds of millions of its users but had stored them as plain text in an internal database that could be accessed unencrypted by its staff.
336. The fact that WhatsApp is owned by FB gives experts pause. Though there are as yet no known major breaches of WhatsApp information since FB bought the application in 2014, unlike some other encrypted messaging applications, including Signal, WhatsApp stores the call times, location and other meta-information of its user's chats, which means they're held by FB.
337. WhatsApp co-founder Brian Acton, who sold WhatsApp to FB, suggested everyone should delete their FB accounts because of FB's many privacy scandals.
338. Left unchecked, FB will play a major role in continuing to spread the sort of propagandistic disinformation, misinformation and propagandistic messaging and advertising that breeds anti-democratic activity in the U.S. and an exponential increase in violence as groups with opposing political views are thrown a steady diet of hate messages broadcast on the FB platform.
339. Now facing numerous regulatory and prosecutorial investigations as well as numerous public and private lawsuits as a result of violating its user's privacy and free

speech rights and its monopolistic practices, FB's recent SEC filing provides an interesting look at just how serious FB is treating the recent round of federal and state lawsuits as so significant they have disclosed them in the company's quarterly SEC report.

340. In a section of a FB SEC filing entitled "Legal Proceedings," FB states: "Beginning on March 20, 2018, multiple putative class actions and derivative actions were filed in state and federal courts in the U.S. and elsewhere against us and certain of our directors and officers alleging violations of securities laws, breach of fiduciary duties, and other causes of action in connection with the misuse of certain data by a developer that shared such data with third parties [...] the events surrounding this misuse of data became the subject of U.S. Federal Trade Commission and other government inquiries in the U.S., Europe, and other jurisdictions. Any such inquiries could subject us to substantial fines and costs, divert resources and the attention of management from our business, or adversely affect our business."

341. However, willfully omitted from that FB statement are: FB's corrupt for-profit role in aiding and abetting Putin-led Russian operatives, the Trump Campaign, Cambridge Analytica, Robert Mercer and others in the malicious cyber-sabotage of the 2016 U.S. presidential elections; that prosecution for such aiding and abetting could lead to FB's shutdown and/or huge penalties and the prospect of imprisonment of the major U.S.-based FB executives involved of the 2016 malicious cyber-sabotage operations.

342. Using the technical and financial resources of FB, Cambridge Analytica, Robert Mercer, the Trump Campaign and others unlawfully obtained Plaintiff's FB user information and that of their FB "Friends" from FB's information repositories and used it to strategically target propagandistic messaging, misinformation, disinformation, lies and other fabrications over the FB platform to boost Trump's candidacy and in so doing directly, recklessly and unlawfully helped sabotage of the 2016 U.S. presidential elections.

343. Proof that Americans who voted for Trump encountered propagandistic messaging far more often than the general voting population follows.

344. When Trump supporters were asked if the future 2020 presidential election should be postponed until the country can make sure that only eligible American citizens can vote, would you support or oppose postponing the election? (1) A majority of the 650-Trump-supporting Republicans surveyed said yes; (2) close to half thought the President had won the popular vote, which he lost by millions of votes; (3) more than two-thirds believed that millions of illegal immigrants had voted, which never happened; and (4) that voter fraud happens regularly, when in fact voter fraud is extremely rare, but election rigging by Russians to favor Trump is not. See *Messing with the Enemy, Surviving in a Social Media World of Hackers, Terrorists, Russians and Fake News* by Clint Watts.

345. FB clawed its way to monopoly market power by fraudulently inducing billions of people, including Plaintiffs, to use the FB platform, never realizing that FB's offer of that purportedly free service was not free because FB fraudulently intended to sell, trade and

otherwise make available to third parties Plaintiff's FB user' information and that of their FB "Friends," and that FB's contractual promises to protect Plaintiff's information nothing but an outrageous and continuing lie.

346. Ultimately, Plaintiff's plundered FB user' information and that of Plaintiff's FB "Friends" would be used by FB, the Trump Campaign, Robert Mercer, Russian intelligence agents and operatives and others to sabotage the 2016 U.S. presidential elections and is now being used to rig the 2020 presidential elections.

347. Plaintiff had intended to use the FB platform for personal political communications and to promote the sale of his political and non-political books.

348. But, FB blocked Plaintiff's unfettered access to his FB personal and business accounts, making it impossible for Zimmerman to delete his information from FB's computer files, or to know how his information was being used by third parties, or to market his books especially *Fair Warning*, *The American Challenge*, *Common Sense* and political ideas using the FB platform or to respond to thousands of messages from his FB "friends."

349. Plaintiff Zimmerman alleges his FB accounts were blocked because his non-violent progressive political views ran counter to those of FB,, who later showed their anti-democratic political ideology when they, along with the Trump Campaign, Robert Mercer, Russian intelligence agents and operatives and others sabotaged the 2016 U.S. political elections in favor of candidate Trump.

350. FB was paid in part in rubles by Russian operatives and allowed those operatives to broadcast hundreds of millions of propagandistic messages, mostly disinformation, misinformation, lies and other fabrications that aggressively promoted the sale of anti-democratic books and hate messaging to hundreds of millions of unsuspecting prospective American voters.

351. It is unlikely that Plaintiffs will ever learn just how many third parties have collected and have used their FB user' information, or will use it in the future, or why FB shut Plaintiffs' accounts down while encouraging the unlawful propagandistic messaging of Russian intelligence agents and operatives, Robert Mercer, the Trump Campaign and others.

352. On or about May 21, 2018, FB began running ads on U.S. national television, and possibly elsewhere, promising to take steps to protect the privacy of its user's FB information.

353. However, to date, these FB promises, like many other of FB's prior promises, were empty promises as FB has not taken any substantive steps to preclude Robert Mercer or the Trump Campaign or Russian operatives or others from the future sabotage of U.S. elections using the FB platform or from using already misappropriated FB user' information for whatever future purposes they wish.

354. Two Russian cyberwarfare operatives described the effects of their cyberwarfare activities stating: "The mass media today can stir up chaos and wreak havoc and

confusion in government and military management of any country and instill ideas of violence, treachery, and immorality, and demoralize the public.

355. Put through this propagandistic onslaught, the U.S. armed forces and the public generally will not be ready with active defenses.” See pp 136-137 in the *Plot to Destroy Democracy* by Malcomb Nance.

356. Putin-led Russian intelligence agents and operatives make no distinction between war and peace as they upped their cyberwarfare activities during the 2016 U.S. presidential cycle and aggressively undertook and continue to undertake strategic subversive tasks aimed at disorienting U.S. voters, sabotaging our elections and destabilizing our governmental institutions and the rule of law.

357. FB Chief Security Officer Alex Stamos testified to Congress that Russian propaganda and Robert Mercer’s far-right political ads were broadcast to approximately 150 million FB users during the 2016 U.S. presidential election cycle, most of which were targeted at key swing states.

358. Stamos said he repeatedly confronted FB executives over the lack of security protecting the FB platform and once told his FB security team that he explained to FB’s top executives that FB has “the threat profile of a Northrop Grumman or a Raytheon or another defense contractor, but we run our corporate network like a college campus.”

359. In 2010, the U.S. Supreme Court lifted restraints on how much money wealthy donors such as Robert Mercer may spend to influence election outcomes, and by 2014 the Mercer Foundation had distributed \$70 million in donations, mainly to extremist right-

wing hate groups, a prime example of the utter destruction of the American foundational principle, “one person, one vote.”

360. Robert Mercer, a reclusive, anti-establishment, extremist right-wing political operative used his wealth and Cambridge Analytica to help candidate Trump win the presidency in return for future presidential favors.

361. Mercer became co-CEO of hedge fund Renaissance Technologies LLC in November 2009 just as the federal government began cracking down on abuses that had contributed to the nation’s worst financial crisis since the Great Depression.

362. In 2010, the IRS issued a public memorandum warning hedge funds and banks about using “basket options.” The memo said that hedge funds should pay taxes at a capital gains rate.

363. Some hedge funds and banks stopped using “basket options,” but not Mercer’s Renaissance.

364. In July 2014, Senator Carl Levin, Chairman of the Senate Investigations Subcommittee and Senator John McCain, issued a report accusing Renaissance of a giant tax dodge on hundreds of millions of option trades and in 2015 the IRS issued a notice to Renaissance, stating that the world’s most profitable hedge fund owed at least 6.8 billion dollars in back taxes.

365. Since then, Mercer has mounted relentless assaults on the IRS, on President Barack Obama, on the SEC, on the Federal Reserve Bank, on the DOJ, on moderate



members of Congress, on presidential candidate Hillary Clinton and on governmental regulations and agencies that negatively-impact Mercer's energy investments.

366. Mercer has called the Civil Rights Act of 1964 a mistake and has voiced disdain for other federal measures to protect the rights of African Americans and other minorities.

367. The Mercer foundation gave nearly \$11 million from 2011 to 2014 to the Media Research Center, an advocacy group whose "sole mission," according to its website, "...is to expose and neutralize the propaganda arm of the Left: the national news media."

368. According to data from the Center for Responsive Politics, Mercer donated more than \$22 million to extremist right wing political candidates, while advocating the abolition of the IRS and much of the federal government.

369. By 2016, Mercer was the leading multi-million-dollar Republican donor to candidate Trump, which helped give Mercer a leading voice in the politics that have impacted all Americans and America's role as a world leader.

370. Some of Mercer's projects sought to unseat his Republican moderates, such as Senator John McCain, who became the target of negative ad campaigns during the 2016 U.S. primary presidential election cycle and also a target of extremely disrespectful Trump tantrums that declared that McCain was no hero because he was captured and draft dodger Trump said he didn't like soldiers that were captured.

371. Meanwhile, Mercer's daughter Rebekah accumulated so much political clout she has been credited with influencing Trump's choices of several top advisors and

appointees, including Steve Bannon, Jeff Sessions, Kellyanne Conway and General Michael Flynn, now a convicted felon.

372. In January 2017, Rebekah Mercer attended a private meeting in which she had secret communications with Jay Clayton, who the President had appointed to chair the SEC, the agency that regulates hedge funds.

373. The Mercers' struggle with the IRS didn't end with Trump's election and Clayton's appointment.

374. Richard Painter, chief White House ethics adviser under President George W. Bush, said the optics surrounding the Mercers' political connections and the IRS case against Renaissance "are terrible. The guy's [Mercer] got a big case in front of the IRS," said Painter, now a University of Minnesota law professor who is also vice chairman of Citizens for Responsibility and Ethics in Washington. "He's trying to put someone in there who's going to drop the case. Is President Trump going to succumb to that or is he not? Are we going to have a commissioner of the IRS who aggressively enforces the law and takes good cases to Tax Court or (somebody who) just throws away tax cases so billionaires don't have to pay their taxes and the rest of us can pay more taxes?"

375. On March 29, 2017, at least 30 conservative leaders, including a Heritage Foundation representative, converged on the White House for an off-the-record meeting with White House officials and pressed for a range of agendas, especially urging the firing of IRS officials not sympathetic to the tax travails of Mercer's Renaissance hedge fund.

376. The meeting was organized by White House aide Paul Teller, who worked with Rebekah Mercer on Senator Cruz's failed 2016 Republican presidential primary campaign, an effort that Mercer backed with \$13.5 million in donations to an independent, pro-Cruz super PAC freed of the usual contribution limits.

377. Robert Mercer then gave millions of dollars more to the super PAC when it began to support candidate Trump.

**VII. SERIOUS DANGERS INHERENT IN FB'S UNREGULATED AND UNACCOUNTABLE MONOPOLISTIC BUSINESS MODEL**

378. Plaintiffs repeat and re-allege all preceding and following paragraphs as if fully set forth herein.

379. FB has falsely promoted itself to its billions of registered users and non-users as an egalitarian "social networking platform" when in fact FB is an authoritarian Internet-based online advertising platform from which FB yearly derives over \$60 billion in advertising and advertising related revenue.

FB uses its monopoly market and political power to advance its self-interested objectives without concern to the harm it is causing.

380. Recently, the FTC and FB agreed on a \$5 billion fine that would settle the FTC's investigation into FB's user privacy violations and other unlawful conduct.

381. FB reported \$15 billion in revenue in a recent quarter, so the \$5 billion fine would amount to a mere one month's revenue.

382. The FTC voted 3-2 to approve the settlement this week, with three yes votes from Republican commissioners and two no votes from Democrats, the *Wall Street Journal* reported today.. Democrats on the commission were "pushing for tougher oversight," the *Journal* reported.

383. "The matter has been moved to the Justice Department's civil division, and it is unclear how long it will take to finalize," the *Journal* reported. Justice Department reviews are part of the FTC's procedure but typically don't change the outcome of an FTC decision."

384. The settlement is expected to include other government restrictions on how FB treats user privacy.

385. FTC officials have also discussed whether to hold Zuckerberg and Sandberg personally accountable, including criminal charges.

386. The FTC investigation began in March 2018 after revelations that up to 87 million users' information was improperly shared with Cambridge Analytica, a political consulting firm that work on the 2016 Trump Campaign. The investigation focused on whether FB violated the terms of its 2011 settlement with the FTC, which prohibited FB from misrepresenting the privacy or security of user information and required FB to get consumers' express consent before making changes that override their privacy settings.

387. Two U.S. Senators found the settlement lacking. "This reported \$5 billion penalty is barely a tap on the wrist, not even a slap," Senator Richard Blumenthal said in a statement. "Such a financial punishment for purposeful, blatant illegality is chump

change for a company that makes tens of billions of dollars every year. Will FB be compelled to alter its present, systematic abuse of privacy? Based on the reported settlement, the answer is sadly, no."

388. Senator Ron Wyden agreed. "Despite Republicans' promises to hold big tech accountable, the FTC appears to have failed miserably at its best opportunity to do so," Wyden said. "No level of corporate fine can replace the necessity to hold Zuckerberg personally responsible for the flagrant, repeated violations of Americans' privacy. That said, this reported fine is a mosquito bite to a corporation the size of FB."

389. FB has willfully failed to enforce its contractual promise to Plaintiffs to protect the privacy of their FB user' information and that of their FB "Friends" by selling and trading that information to third parties and by allowing still other third parties free ,unfettered access to that information to use in any way that they see fit.

390. Hundreds of millions of Americans use the FB platform for countless purposes including advertising their goods and services, as an adjunct or alternate to email, to view and/or promote news and to broadcast their personal opinions on every conceivable topic.

391. FB denied Plaintiffs unfettered access to their FB accounts for no expressed legitimate reason but continued to allow their FB "Friends" and others to send them messages and continued to amass, sell, trade, supplement and aggregate their FB user' information.

392. On June 29, 2018, FB provided written responses to seven hundred questions put to them by the U.S. House of Representatives. In providing answers to these questions, FB

identified certain of the types of information its collects, stores, supplements, aggregates, sells and trades, including:

393. ● Device attributes such as operating systems, hardware and software versions, battery level, signal strength, available storage space, browser type, application and file names and types, and plugins.
394. ● Device operation information and behaviors performed on the device, such as whether a window is foregrounded or backgrounded and mouse movements (used to distinguish humans from bots).
395. ● Unique device IDs, and other identifiers, such as from games, applications and accounts people use, and family device IDs (or other identifiers unique to FB products associated with the same device or account).
396. ● Device signals and information about nearby Wi-Fi access points, beacons, and cell towers.
397. ● Information from device settings such as unfettered access to FB user' GPS locations, cameras and photos.
398. ● Network and connection such as the name of user's mobile operator or ISP, language, time zone, mobile phone number, Internet provider address, connection speed and, in some cases, information about other devices that are nearby or on user's network, so we can do things like help people stream a video.
399. ● Cookie information stored on a FB user's device, including cookie IDs and settings.

400. FB has willfully and unlawfully allowed unfettered access to and sold or traded to all sorts of third parties, application developers and device manufacturers unfettered access to Plaintiff's FB user' information and that of their FB "Friends" while denying Plaintiffs the ability to change or delete that information.

401. An example of FB's failure to enforce its contractual promise to protect from access and use and sale by third parties came to light when it was discovered in the mid-2010s that FB allowed a Cambridge University researcher unfettered access to FB user' information from nearly a hundred million FB's users and their FB "Friends," one of many FB willful, reckless and unlawful failures to protect the privacy of FB user' information.

402. In 2014, that Cambridge University researcher entered into a contract with Robert Mercer controlled Cambridge Analytica for the sale of the researcher's plundered FB user' information for approximately \$\$800,000.

403. The plundered FB user' information was then repeatedly used by FB, the Trump Campaign, Russian operatives, Cambridge Analytica, Robert Mercer and others in a successful effort to sabotage the primary and general 2016 U.S. presidential elections in favor of candidate Trump.

404. The unlawful and possibly treasonous conduct of, FB, the Trump Campaign, Russian operatives, Cambridge Analytica, Robert Mercer and others could have been thwarted had if FB had denied the Cambridge University researcher's application to FB to access and use FB-stored user' information.

405. Cambridge Analytica received millions of dollars from the Trump Campaign and other 2016 U.S. presidential candidates for the use of its plundered FB user' information and the technical services of Cambridge Analytica employees who became embedded along with FB employees in Trump Campaign information processing facilities and assisted in the Trump Campaign's efforts to rig U.S. 2016 presidential elections in favor of Trump.

406. FB also granted licenses to Blackberry and at least 52 other device manufacturers that allowed the device manufacturers to integrate their devices with FB.

407. These integrations gave the device manufacturers through applications like Blackberry's "HUB unfettered access to unlimited quantities of FB user' information, leaving FB users with no control over how their information was accessed and then used or sold or traded.

408. Even if FB users had denied such access, their denials were easily circumvented with the full knowledge, consent and encouragement of FB.

409. FB's willful misrepresentations to its users and failure to inform their users, including Plaintiffs that their information was being compromised willfully and recklessly deceived Plaintiffs and caused them monetary and emotional harm.

410. Using the plundered FB user' information of nearly a hundred million Americans, including that of the Plaintiffs, and thousands of emails plundered from the Democratic National Committee ("DNC") and the Democratic Congressional Campaign Committee ("DCCC"), FB, working in concert with Russian intelligence agents and operatives, the



Trump Campaign, Cambridge Analytic, Robert Mercer and others successfully rigged the 2016 U.S. presidential elections in favor of candidate Trump.

411. Zimmerman is not a public official, or public figure, or a candidate for public office, or a campaign official, or a personal advisor to any political candidate and did not expect his FB user' information or that of his FB "Friends" would become available to anyone who wanted it to use for any purpose whatsoever.

412. To repeat, FB contractually promised Plaintiffs and billions of other registered FB users that their FB user' information would be protected from unauthorized access and use by third parties.

413. Approximately 60% of Americans are or have been registered FB users.

414. FB has profited by tens of billions of dollars selling and trading FB user' information and selling ads that were strategically targeted to exploit the personality traits and other personal private information of Zimmerman and millions of other FB users.

415. The Trump Campaign spent at least \$44 million on strategically targeted FB ads from June 2016 to November 2016 and continues such targeted messaging on the FB platform in its 2020 presidential reelection campaign.

416. Strategic ad targeting was used by Trump supporter and major donor Robert Mercer to help sabotage the 2016 U.S. presidential election cycle.

417. Robert Mercer along with the President's former senior advisor Steve Bannon, controlled, *Breitbart News*, a publication that advances what the *New York Times* calls "'hate news'" (a toxic mix of lies, white-supremacist content, and bullying that have inspired

attacks on Muslims and their mosques, gay people, women, African Americans and their churches, Jewish people and their synagogues and others).

418. In 2016, employees of FB, the Trump Campaign, Cambridge Analytica and others joined Trump's senior advisor Jared Kushner in a San Antonio-based information processing facility and deployed the voter profiles of millions of Americans plundered from FB to successfully sabotage the 2016 U.S. presidential elections.

419. Kushner has been under investigation for his undisclosed contacts with Russian ambassador Sergey Kislyak, the CEO of a U.S. sanctioned Russian bank and others.

420. FB announced that about 25% of the ads purchased by Russian operatives from FB during the 2016 U. S. presidential elections were "geographically targeted," meaning that they played primarily in swing states.

421. In a 2016 post-election interview, Kushner told *Forbes* magazine that he had been keenly interested in FB's microtargeting capability. "I called somebody who works for one of the technology companies that I work with, and I had them give me a tutorial on how to use FB micro-targeting," Kushner said. Adding, "We brought in Cambridge Analytica. I called some of my friends from Silicon Valley who were some of the best digital marketers in the world," Kushner said, "And I asked them how to scale this stuff . . . We basically had to build a \$400 million [voter targeting] operation with 1,500 people operating in 50 states."

422. By willfully, recklessly and for profit abdicating its contractual responsibility to protect the privacy of Plaintiff's FB user' information from unauthorized and/or unlawful

invasions of his privacy, FB willfully and recklessly allowed Cambridge Analytica and numerous other third parties to plunder and use for unlawful purposes vast amounts of their FB user' information without FB user' consent, including Plaintiff's.

**VIII. FB'S USE OF ITS USERS' INFORMATION AS AN EXTREMELY VALUABLE ASSET WHEN NEGOTIATING DEALS WITH THIRD PARTIES TO GAIN UNFETTERED ACCESS TO IT**

423. Plaintiffs repeat and re-allege all preceding and following paragraphs as if fully set forth herein.

424. According to some 4,000 pages of leaked FB documents spanning 2011 to 2015 obtained by *NBC News*, Zuckerberg supervised plans to consolidate FB's ability to out-compete competitors by treating its FB user's information as an extremely valuable asset when negotiating deals to gain unfettered access to it with third parties, while publicly proclaiming to be protecting the privacy of that very same FB user' information.

425. The leaked documents, which include emails, webchats, presentations, spreadsheets and meeting summaries, show how FB, along with FB's board of directors and management team, found ways to tap FB's trove of FB user' information, including information about FB "Friends," relationships, photos and videos, as leverage over companies it had partnered with.

426. In some cases, FB would reward favored FB partnered companies by giving them unfettered access to the information of its users. In other cases, it would deny user-information unfettered access to rival companies.

427. For example, FB gave Amazon extended unfettered access to FB user' information because it was spending money on FB advertising and partnering with FB on the launch of its "Fire" smartphone.
428. FB also discussed cutting off unfettered access to FB user' information for a messaging application that was viewed by FB executives as a too popular competitor.
429. Private communication between users is "increasingly important," Zuckerberg said in a 2014 *New York Times* interview. "Anything we can do that makes people feel more comfortable is really good." But leaked FB documents show that secretly, contrary to FB's public statements, FB conjured up ways to require third party applications to compensate FB for unfettered access to its FB user's information, including direct payment, advertising spending and information-sharing arrangements.
430. Ultimately FB decided not to sell the information directly but rather to dole it out to application developers who were considered personal friends of Zuckerberg and/or Sandberg or who spent big money on FB ads like Amazon and/or shared their own customer information with FB.
431. About 400 of the 4,000 leaked FB pages of the leaked documents had been previously been disclosed. However, the previously undisclosed leaked documents convey the most comprehensive insight into FB's deceptive and unlawful activities while the company struggled to adapt to the rise of smartphones following its scratchy debut as a public company in 2012.

432. The thousands of previously undisclosed FB leaked documents were anonymously leaked to the British investigative journalist Duncan Campbell, who shared them with a handful of media organizations such as *NBC News*, *Computer Weekly* and *Süddeutsche Zeitung*.

433. FB has not questioned the authenticity of the leaked FB documents, each of which was presented as evidence in a California court case between FB and a startup company called Six4Three that sued FB in 2015 after FB announced plans to cut off their unfettered access to FB user' information.

434. The Six4Three's computer application, called Pikinis, was launched in 2013 and relied on FB user' information to find photos of persons clothed only in bathing suits.

435. According to the *Wall Street Journal*, FB has admitted that it considered charging for unfettered access to FB user' information, but found there were better ways to monetize unfettered access to its users' information.

436. In a preliminary decision, the judge in the Six4Three case found "evidence of FB's fraudulent conduct.

437. The leaked documents show that FB's plans to sell unfettered access to FB user' information received support from FB's most senior executives, including CEO Zuckerberg, COO Sheryl Sandberg, Chief Product Officer Chris Cox and Vice President of growth Javier Olivan.

438. When in 2015 FB discontinued unfettered access to FB user' information for certain third parties, that FB action contributed to the decline of Pikinis, Lulu, and Beehive .

439. One of the most striking examples of FB's willful misconduct to emerge from the leaked documents is the way that FB user' information was traded to squeeze money or shared information from third party application developers.

440. In the wake of the Cambridge Analytica scandal and rising awareness of the Six4Three lawsuit, FB attempted to spin the modest changes it made to its platform in 2014 and 2015 as major events and as being driven by FB concerns over user privacy.

441. However, the leaked documents show that protecting FB user' privacy was not a major concern for FB, and the issue was rarely discussed in the thousands of pages of leaked emails and meeting summaries.

442. When FB user' privacy was mentioned, it was in the context of how FB can use it as a public relations strategy to soften the blow of the sweeping changes to application developer's unfettered access to FB user' information. The leaked documents include several examples suggesting that these changes were designed to cement FB's power in the marketplace, not to protect users.

443. Early on, FB recognized that working with and helping third party application developers with free unfettered access to FB user' information, would make FB more interesting and accelerate FB's growth.



444. Beginning in early 2010, FB created tools that allowed makers of computer games and other applications to connect with FB users so that FB users would spend more time using the FB platform and managed to achieve this through its Graph API (Application Programming Interface) that allowed software programs to interact with each other.

445. In FB's case, this meant that third party applications such as online computer games could post updates on FB user' profiles, which would be seen by computer game player's FB "Friends" and tempt them to play as well and allow game creators to access information from FB users, including their connections to FB "Friends," FB "Likes," locations, updates, photos and more.

446. Graph API, and particularly the way it let third parties promote their products and extract information from a FB user's "Friends," was a key feature of FB that Six4Three and thousands of other companies relied upon.

447. However, a few years later, FB decided the application developers were getting more value from their unfettered access to FB user' information than FB was getting from the application developers.

448. Soon after FB sold a wee portion of its stock to the public, the rapid growth of the cellphones threatened FB's market power and growth and an internal FB presentation looking back at this period used the phrase "terminal decline" to describe the fall in FB user engagement.



449. Zuckerberg, Sandberg and other FB executives spent months brainstorming ways to exploit the explosive growth of cellphone use before that explosively expanding market got away from them.
450. One idea that FB kept returning to was to make money from FB's application developer partners by charging them for unfettered access to FB's users and their information.
451. Several proposals for charging application developers for unfettered access to FB's platform and FB user information were put forward in a presentation to the company's board of directors.
452. Among the suggestions: a fixed annual fee for application developers for reviewing their applications; an access fee for applications that requested FB user' information; and a charge for "premium" unfettered access to FB user' information, such as a user trust score or a ranking of the strongest relationships between FB users and their FB "Friends."
453. "Today the fundamental trade is 'information for distribution,' whereas we want to change it to either 'information for \$' and/or '\$ for distribution,'" a FB business development director wrote in an August 2012 internal email.
454. Such discussions continued through October 2012, when Zuckerberg explained to close friend Sam Lessin the importance of controlling third party application's ability to access FB's user' information and reach FB user's "Friends" on the FB platform.

455. Without that leverage, “I don’t think we have any way to get application developers to pay us at all,” Zuckerberg wrote in an email to Lessin.
456. Then Zuckerberg suggested pursuing 100 deals with application developers “as a path to figuring out the real market value of FB user’ information and then setting a public rate for application developers. “The goal here wouldn’t be the deals themselves,” said Zuckerberg, “...but that through the process of negotiating with them we’d learn what application developers would actually pay, which might be different from what they’d say if we just asked them about the value, and then we’d be better informed on our path to set a public rate.”
457. As usual, Zuckerberg ignored the potential privacy risks associated with FB’s user information-sharing arrangements. “I’m generally skeptical that there is as much information leak strategic risk as you think,” he wrote in the email to Lessin. “I think we leak info to developers, but I just can’t think of any instances where that information has leaked from developer to developer and caused a real issue for us.” But, the following year, a privacy defect affecting a third party application developers created precisely that sort of issue for FB, as depicted in a panicky chatlog between Michael Vernal, who was FB’s director of engineering, and other senior FB employees.
458. Apparently, Zuckerberg’s private communications were leaked from FB to an external application in an unexpected way.

459. Vernal said that it could have been near-fatal for the FB if Zuckerberg had accidentally disclosed earnings ahead of time because a FB sanctioned application had intruded on his privacy.

460. “Holy crap,” replied Avichal Garg, then director of product management. “DO NOT REPEAT THIS STORY OFF OF THIS THREAD,” added Vernal. “I can’t tell you how terrible this would have been for all of us had this not been caught quickly.”

461. In late November 2012, Zuckerberg sent a long email to FB’s senior executives stating FB should not charge application developers for unfettered access to FB user’ information.

462. However, Zuckerberg also said that unfettered access to FB user’ information should be contingent on the application developers sharing all of the “social content” generated by their applications with FB, something Zuckerberg called “full reciprocity.”

463. The existing arrangement, where application developers weren’t required to share their information with FB, might be “good for the world, but it’s not “good for us,” Zuckerberg wrote in an email and added that “...though FB could charge application developers to access FB user’ information, FB stood to benefit more from requiring application developers to compensate FB by sharing their customer information and by buying advertising on FB’s platform.

464. FB began making deals with some of its most valued partners, including dozens of application developer friends of Zuckerberg and Sandberg by “whitelisting” their

unfettered access to FB user' information while restricting unfettered access to application developers FB determined were competitors.

465. These FB negotiated information access deals with key FB business partners, including Tinder, Sony, Amazon and Microsoft, required sweeping changes to the FB platform, changes FB planned to announce at its annual application developer conference in April 2014.

466. in June 2013I, leaked FB documents described that Amazon received special treatment for the launch of a group gifting product, despite the fact that it competed with one of FB's own products.

467. "Remind me, why did we allow them [Amazon] to do this? Do we receive any cut of purchases?" Chris Daniels, then FB's director of business development, asked in an email.

468. "No, but Amazon is an advertiser and supporting this with advertisements ... and working with us on deeper integrations for the Fire," Amazon's smartphone, replied Jackie Chang, who worked with FB's strategic business partners.

469. Amazon released a statement to *NBC News*: "Amazon uses publicly available APIs provided by FB in order to enable FB experiences for our products and only uses information in accordance with our privacy policy." An admission that Amazon had collected and stored FB user' information for its own use and profit and that that information was now subject to Amazon's customer information policies.



470. The applications of application developers that were not considered “strategic partners” got less favorite nation status treatment from FB.
471. In a March 2013 discussion, Justin Osofsky, then director of FB platform business partnerships, described restricting the MessageMe application from unfettered access to FB user’ information because it had grown too popular and could compete with FB messages.
472. Osofsky asked his staff to see if any other messenger applications have “hit the growth team’s radar recently.” “If so, we’d like to restrict them at the same time to group this into one press cycle," he wrote in an email.
473. The FB driven deal negotiations created confusion among FB’s business partners who had grown accustomed to unfettered access to FB user’ information.
474. “We gave a bunch of stuff for free historically (information, distribution) and now we’re making you ‘pay’ for it via reciprocal value,” Vernal, director of FB engineering, wrote in an email in June 2013. He added, “The confusing thing here is that we haven’t really announced these changes publicly/broadly yet.”
475. Some FB employees were unhappy about this direction, particularly the way FB appeared to be blocking competitors from unfettered access to FB user’ information.
476. Following is an extract from a December 2013 chatlog between several FB senior engineers talking about the changes to application developers’ unfettered access to FB user’ information:

477. Bryan Klimt: “So we are literally going to group applications into buckets based on how scared we are of them and give them different APIs? ... So, the message is, ‘if you’re going to compete with us at all, make sure you don’t integrate with us at all’? I’m just dumbfounded.”

478. Kevin Lacker: “Yeah this is complicated.”

479. David Poll: “More than complicated, it’s sort of unethical.”

480. When it came to announcing the sweeping changes at FB’s annual F8 application developer conference in April 2014, members of the communications team worked with Zuckerberg to craft a narrative around FB user’ trust, not competition or profitability.

481. In a March 2014 email discussing Zuckerberg’s keynote speech at FB’s annual F8 application developer conference, where he was due to announce the removal of application developer’s unfettered access to FB “Friends” information, Jonny Thaw, a FB director of communications, wrote that it “may be a tough message for some application developers as it may inhibit their growth.”

482. One idea that came up was talking in the keynote about some of the trust changes we’re making on FB itself. So, the message would be: ‘trust is really important to us, on FB we’re doing A, B and C to help people control and understand what they’re sharing and with platform applications we’re doing D, E and F. If that doesn’t work,” he added, “we could announce some of FB’s trust initiatives in the run up to F8 to make the changes for application developers seem more natural.”

483. FB user trust was crucial when Zuckerberg delivered his keynote speech at the F8 conference on April 30, 2014, where Zuckerberg said: “Over the years, one of the things we’ve heard over and over again is that people want more control over how they share their information, especially with applications, and they want more say and control over how applications use their information,” he told the audience of journalists and application developers. “And we take this really seriously because if people don’t have the tools they need to feel comfortable using your applications, that’s bad for them and that’s bad for you.”

484. But despite FB’s purported focus on user privacy, FB staff member emails described confusion over the way third party applications could override user’s privacy settings.

485. Even if FB users locked down their account so that their photos and other FB user’ information were visible to “only me,” those photos were still accessible by third parties.

486. In April 2015, Connie Yang, a FB product designer, told her colleagues that she’d discovered applications collecting FB profile information she had marked as “only me” and displaying it to “both you and other people using that application.”

487. Even though FB eventually decided against charging application developers directly for unfettered access to FB user’ information, one of the biggest threats FB now faced was not competition from application developers, but rather from federal antitrust regulation.



488. Eventually, the FTC announced a task force to monitor anti-competitive behavior in the technology industry to, in the words of FTC chair Joseph Simons, “...ensure consumers benefit from free and fair competition.”

489. Congressional lawmakers started pressuring the FTC to investigate FB for antitrust violations.

490. David Cicilline, chairman of the House Judiciary Antitrust Subcommittee, wrote in a *New York Times* op-ed: “FB appears to have used its [market] dominance to cripple other competitive threats by cutting them off from its massive network.”

491. Trying to appease Congress and the FTC, a Zuckerberg op-ed appeared in the *Washington Post* in March 2018 calling for some regulation in such areas as election sabotage, but not antitrust punishment.

492. Ashkan Soltani, a privacy expert and former FTC chief technologist, said that Zuckerberg is approaching the looming threat of regulation with “bravado” and trying to “leverage things for his benefit.”

493. Zuckerberg and other senior FB executives are now being investigated by Congress, governmental regulators and prosecutors domestic and foreign, as well as defending against numerous private party information privacy violation lawsuits.

494. In 2018, Zuckerberg told Congress that he’s responsible for what happens at FB.

495. Senator Richard Blumenthal, who recently criticized the FTC for taking too long on the FB probe, wants the FTC to hold Zuckerberg accountable.

496. But Zuckerberg is accountable to no person and no government regulatory agency. His power over what FB does and doesn't do is absolute.
497. In late May 2019, FB investors voted overwhelmingly in support of proposals to fire Zuckerberg as chairman and scrap the firm's stock share structure. According to the results of votes at FB's annual shareholder meeting 68% of outside investors want the company to hire an independent chairman, up from 51% in 2018.
498. Despite the vote, the management and share restructuring proposals did not pass because of Zuckerberg has voting control by virtue of his majority stock holdings, which means he can and does ignore outside shareholder demands.
499. "Arrogance is not a substitute for good corporate governance," said Michael Connor, who helped coordinate action among activist FB investors.
500. Senator Blumenthal told the *Washington Post*. "Holding Mark Zuckerberg and other top FB executives personally at fault and liable for further wrongdoing would send a powerful message to business leaders across the country: You [Zuckerberg] will pay a hefty price for skirting the law and deceiving consumers."
501. In 2018, in a purported act of contrition, Zuckerberg told the House Committee on Energy and Commerce: "But it's clear now we [FB executives] didn't do enough to prevent these tools [the FB platform and application and algorithms] from being used for harm as well. That goes for fake news, foreign interference in elections and hate speech, as well as developers and data privacy. We didn't take a broad enough view of our



responsibility and that was a big mistake. It was my mistake, and I'm sorry. I started FB. I run it, and I'm responsible for what happens here [at FB].”

**IX. RUSSIAN "ACTIVE MEASURES" DEPLOYED TO SABOTAGE THE 2016 U.S. PRESIDENTIAL ELECTIONS USING THE FB PLATFORM AS SET OUT IN THE SPECIAL COUNSEL'S REDACTED REPORT**

502. Plaintiffs repeat and re-allege all preceding and following paragraphs as if fully set forth herein.\

503. The first form of Russian election sabotage came principally from the Russian Internet Research Agency (Russian IRA), an organization funded by Yevgeniy Viktorovich Prigozhin and companies he controlled, including Concord Management and Consulting LLC and Concord Catering (collectively "Concord").

504. The Russian IRA conducted election sabotage operations using the FB platform targeted at prospective U.S. voters in a successful effort to sow discord among them that resulted in in the successful sabotage of the U.S. 2016 presidential election cycle.

505. These operations constituted "active measures" (*aKTMBHbMie eporrprumu1*), a term that refers to operations conducted by Russian security services aimed at influencing the course of international affairs.

506. The Russian IRA and its employees began operations targeting the U.S. in 2014, possibly earlier.

507. Using fictitious U.S. personas, Russian IRA employees operated FB accounts and FB group pages with the intent to influence U.S. voters. These FB groups and FB

accounts, which addressed divisive U.S. political and social issues, falsely claimed to be controlled by U.S. persons.

508. Multiple Russian IRA controlled FB groups and other Russian entities engaged in similar “active measures” election sabotage operations targeting prospective U.S. voters

509. Over time, these Russian IRA-controlled FB accounts and other Internet-based platforms became a means to reach ever larger U.S. audiences.

510. Also, Russian IRA employees travelled to the U.S. in mid-2014 on an intelligence-gathering mission to obtain information and photographs for use in their FB and other Internet-based platforms.

511. Russian IRA employees posted derogatory information about a number of political candidates in the 2016 U.S. presidential elections and in early to mid-2016 Russian IRA election sabotage operations included supporting the Trump Campaign and disparaging Secretary Clinton’s campaign.

512. The Russian IRA made various expenditures to carry out their election sabotage activities, including buying political advertisements on FB and other social media using fictitious names of U.S. persons and entities.

513. Some Russian IRA employees posing as U.S. persons and without revealing their Russian association communicated electronically with Trump Campaign associates and with other political activists seeking to coordinate pro-Trump political activities.

514. By the end of the 2016 U.S. presidential elections the Russian IRA had reached millions of U.S. persons through their FB and other Internet-based platforms.

515. The Special Counsel’s “active measures” investigation has resulted in criminal charges against 13 Russian nationals and three Russian entities, principally for conspiracy to defraud the U.S., in violation of 18 U.S.C. § 371. See Volume I, Section V.A, *infra*; Indictment, *United States v. Internet Research Agency, et al.*, 1 :18-cr-32 (D.D.C. Feb. 16, 2018), Doc. I (Internet Research Agency Indictment).

516. In November 2017, a FB executive testified that FB had identified 470 Russian IRA-controlled FB accounts that collectively made 80,000 posts between January 2015 and August 2017.

517. FB estimated the Russian IRA reached as many as 126 million persons through its FB accounts.

518. In a hearing before the Senate Select Committee on Intelligence, Colin Stretch, FB’s then General Counsel, estimated that roughly 29 million people were served content in their FB “News Feeds” directly from the Russian IRA’s 80,000 posts over two years.

519. Russian IRA posts from these FB pages were also shared, liked, and followed by people on FB, and, as a result, three times more people were exposed to a story that originated from the Russian U.S. election sabotage operation.

520. FB has estimated that approximately 126 million people were served content from a FB pages associated with the Russian IRA at some point during the 2016 presidential election cycle.

521. The FB general counsel also testified that FB had identified 170 FB-owned Instagram accounts that posted approximately 120,000 pieces of content during the 2016

presidential election cycle but did not offer an estimate of the number of persons reached via FB-owned Instagram.

522. In 2016, Russian IRA employees claiming to be U.S. political activists and administrators of FB groups, recruited U.S. persons to hold signs in front of the White House.

523. In June 2014, four Russian IRA employees applied to the U.S. Department of State to enter the U.S. and lied about the purpose of their trip, claiming to be four "Friends" who had met at a party. Ultimately, two Russian IRA employees-Anna Bogacheva and Aleksandra Krylova-received visas and entered the U.S. on June 4, 2014.

524. Dozens of Russian IRA employees were responsible for operating accounts on FB and were referred to within the agency as "specialists."

525. Russian IRA's operations focused their election rigging efforts on FB, YouTube, and Twitter and later added specialists who operated on Tumblr and Instagram accounts.

526. The Russian IRA-controlled FB groups including "Secured Borders, " the groups "Being Patriotic," "Stop All Immigrants," "Secured Borders," and "Tea Party News"), "Black Matters," "Blacktivist, " "Don't Shoot Us," "LGBT United,") and "United Muslims of America."

527. Throughout 2016, Russian IRA accounts published an increasing number of materials supporting the Trump Campaign and opposing the Clinton Campaign.

528. For example, on May 31, 2016, the operational account "Matt Skiber" began to privately message dozens of pro-Trump FB groups asking them to help plan a pro-Trump rally near Trump Tower.
529. To reach ever larger U.S. audiences, the Russian IRA purchased advertisements from FB that promoted Russian IRA FB groups on the FB newsfeeds of U.S. FB users.
530. According to FB, the Russian IRA purchased over 3,500 advertisements, paying approximately \$100,000, using U.S. currency and Russian rubles.
531. During the 2016 U.S. presidential campaign, numerous Russian IRA-purchased advertisements explicitly supporting or opposing a presidential candidate or promoting U.S. political rallies organized, in part, by the Russian IRA.
532. Starting as early as March 2016, the Russian IRA purchased advertisements on FB that overtly opposed the Clinton Campaign.
533. For example, on March 18, 2016, the Russian IRA purchased an advertisement depicting candidate Clinton in a caption that read in part, " If one day God lets this liar enter the White House as a president - that day would be a real national tragedy."
534. Similarly, on April 6, 2016, the Russian IRA purchased FB advertisements for its account "Black Matters" calling for a "flashmob" of U.S. persons to "take a photo with #HillaryClintonForPrison2016 or #nohillary2016."
535. Russian IRA-purchased FB advertisements referencing candidate Trump supported the Trump Campaign and disparaged Secretary Clinton's campaign.



536. The first known Russian IRA advertisement explicitly endorsing Trump was purchased on April 19, 2016.
537. The Russian IRA bought an advertisement for its FB-owned Instagram account "Tea Party News" asking U.S. persons to help them "make a patriotic team of young Trump supporters " by uploading photos with the hashtag "#KIDS4TRUMP."
538. In subsequent months, the Russian IRA purchased dozens of advertisements supporting the Trump Campaign, predominantly through the FB groups "Being Patriotic," "Stop All Invaders," and "Secured Borders."
539. Collectively, the Russian IRA's social media accounts reached hundreds-of millions of Americans.
540. Individual Russian IRA FB and other platforms attracted hundreds of thousands of followers.
541. For example, at the time they were deactivated by FB after the completion of the 2016 U.S. presidential cycle in mid-2017, the Russian IRA's "United Muslims of America" FB group had over 300,000 followers, the "Don't Shoot Us" FB group had over 250,000 followers, the "Being Patriotic" FB group had over 200,000 followers, and the "Secured Borders" FB group had over 130,000 followers.
542. Moreover, the Russian IRA organized and promoted political rallies inside the U.S. while posing as U.S. grassroots activists, using FB groups and to announce and promote the event.

543. The Russian IRA then sent a large number of direct messages to its FB followers asking them to attend the event. From those who responded with interest in attending, the Russian IRA then sought a U.S. person to serve as the event's coordinator. In most cases, the Russian IRA account operator would tell the U.S. person that they personally could not attend the event due to some preexisting conflict or because they were somewhere else in the U.S.

544. The Russian IRA then further promoted the event by contacting U.S. media about the event and directing them to speak with the coordinator.

545. After the event, the Russian IRA posted videos and photographs of the event to the Russian IRA 's FB accounts.

546. The Special Counsel's redacted report identified dozens of U.S. rallies organized by Russian IRA.

547. The earliest evidence of a rally was a "confederate rally" in November 2015.

548. The Russian IRA continued to organize rallies even after the 2016 U.S. presidential elections.

549. The Russian IRA recruited U.S. persons from across the political spectrum. For example, the Russian IRA targeted a number of black social justice activists.

550. The Russian IRA also recruited moderators of conservative Internet-based groups to promote IRA-generated content, as well as recruited individuals to perform political acts, such as walking around New York City dressed up as Santa Claus with a Trump mask.

551. As the Russian IRA's online audience became ever larger, they tracked U.S. persons with whom they communicated and had successfully tasked with tasks ran in from organizing rallies to taking pictures with certain political messages.
552. With regard to Russian IRA interactions and contacts with the Trump Campaign, the Special Counsel's investigation identified several forms of connections between the Russian IRA and members of the Trump Campaign and no similar connections with the Clinton Campaign.
553. For example, on multiple occasions, members and surrogates of the Trump Campaign promoted, typically by linking, retweeting , or similar methods of reposting pro-Trump or anti-Clinton content published by the Russian IRA through Russian IRA-controlled FB and other platforms.
554. Among the U.S. leaders of public opinion targeted by the Russian IRA were various members and surrogates of the Trump Campaign. In total, Trump Campaign affiliates promoted dozens of tweets, posts , and other political content created by the Russian IRA.
555. In sum, the Special Counsel's investigation established that Russia interfered in the 2016 presidential election through the "active measures" social media campaign carried out by the Russian IRA, an organization funded by Yevgeniy Viktorovich Prigozhin and companies that he controlled.
556. The Special Counsel's redacted report concluded that Prigozhin, his companies and Russian IRA employees violated U.S. law through these operations, principally by

undermining through deceptive acts the work of federal agencies charged with regulating foreign influence in U.S. elections.

557. Moreover, the full extent of FB's participation in the sabotage of the 2016 U.S. presidential elections is as yet unknowable as much of the FB participation has been heavily redacted in the version of the Special Counsel's report released for public consumption and certain aspects of the sabotage exceeded to boundaries set by the DOJ for investigation by the Special Counsel.

## **X. CAUSES OF ACTION**

558. All of the following causes of action are lodged against each of the FB Defendants.

### **COUNT ONE-VIOLATIONS OF THE COMPUTER FRAUD AND ABUSE ACT**

559. Plaintiffs incorporate by reference all paragraphs contained throughout this Complaint as though fully set forth herein.

560. At all relevant times, FB Defendants, FB's Internet-based platform, FB user' information and FB servers were involved in interstate and foreign commerce and communication as covered by 18 U.S.C. § 1030(e)(2) and still are.

561. In direct violation of 18 U.S.C. § 1030, FB Defendants, the Trump Campaign, Cambridge Analytica, Robert Mercer and others willfully and with fraudulent intent used Plaintiff's plundered FB user' information and that of nearly a hundred million other FB users to successfully sabotage the 2016 U.S. presidential elections.

562. The specific FB user' information of Plaintiffs plundered by Cambridge Analytica has not as yet been disclosed by FB or Cambridge Analytica, but that information could have included, but was not necessarily limited to, Plaintiff's individual and company names and addresses, hometowns; birthdates; gender; family connections; educational achievements; email addresses; relationship statuses; work histories; interests; hobbies ;religious and political affiliations; phone numbers; dates and times of active sessions on FB; dates and times and titles of Plaintiff's FB ads; connections and communications with other FB users; attendance at events and social gatherings, stored credit/debit card information, Plaintiffs thousands of FB "Friends" and FB "groups" Plaintiffs belonged to; a list of Internet provider addresses Zimmerman used, posts and/or websites Zimmerman has liked, Google searches conducted Zimmerman and photographs and/or videos.

563. This plundering of Plaintiff's FB user information, and that of nearly a hundred million other FB users, was accomplished, in part, when Robert Mercer funded and then directed Cambridge Analytica to create individual FB user' voter profiles based on demographics, political attitudes, religion, sexual orientation and the like and then together with the Trump Campaign and Russian operatives bombarded prospective 2016 U.S. presidential election voters with pro-candidate Trump and anti-Secretary Clinton disinformation, misinformation, propagandistic political messaging and advertising using the FB platform without a single intervention by FB, even though FB were well aware of this unlawful activity.

564. Instead of blocking the unlawful conduct of the Trump Campaign, Mercer, Cambridge Analytica and Russian operatives, FB and Cambridge Analytica aided and abetted the unlawful conduct by assigning their personal to the Trump Campaign political information processing offices that were used to help that campaign successfully sabotage the 2016 U.S. presidential elections in violation of 18 U.S.C. § 1030(a)(6)(A).

565. Plaintiffs and many others suffered damage and loss and continue to suffer damage and loss as a consequence of FB Defendant's actions, including but not limited to the cost of investigating and responding to the unauthorized access and abuse of their FB user information and that of their "Friends" and therefore seek compensatory and other equitable relief under 18 U.S.C. § 1030(g).

566. As a direct and proximate result of the conduct of FB, Plaintiffs have sustained significant harm, entitling them to damages in an amount to be established at trial.

#### **COUNT TWO-UNJUST ENRICHMENT**

567. Plaintiffs incorporate by reference all paragraphs contained throughout this Complaint as though fully set forth herein.

568. As alleged herein, FB have unjustly received and retained monetary benefits from Plaintiffs by way of its profiting from the use of their FB user' information under unjust circumstances, such that inequity has resulted.

569. By engaging in the conduct described in this Complaint, FB knowingly obtained benefits from Plaintiffs as alleged herein under circumstances such that it would be inequitable and unjust for FB to retain them.

570. More specifically, by engaging in the acts and failures to act described in this Complaint, FB have been knowingly enriched by the savings in costs that should have been reasonably expended to protect the privacy of Plaintiff's FB user' information and by a substantial increase in the share price of FB. See *Restatement (Third) of Restitution and Unjust Enrichment* § 39(1) (2011).

571. Moreover, FB have been enriched unjustly by the use of Plaintiff's information for its advertising business, and has profited greatly as a result, even though it did not protect this information as it had promised.

572. By engaging in the conduct described in this Complaint, FB have knowingly obtained benefits from or by way of Plaintiffs, including by way of the use of their information in the course of its business, especially its lucrative advertising business, under circumstances such that it would be inequitable and unjust for it to retain them.

573. Thus, FB will be unjustly enriched if they are permitted to retain the benefits derived from the unauthorized and impermissible gathering and sharing of Plaintiff's FB user' information by FB authorized and unauthorized third parties.

As a direct and proximate result of the conduct of FB Defendants Plaintiffs have sustained significant harm, entitling them to damages in an amount to be established at trial.

### **COUNT THREE-VIOLATIONS OF CONSTITUTIONAL RIGHTS**

574. Plaintiffs incorporate by reference all paragraphs contained throughout this Complaint as though fully set forth herein.

575. This case is likely one of the first filed in this Court that addresses the relationship between the First Amendment and the Internet-based FB communications platform.

576. A fundamental principle of the First Amendment is that all persons have unfettered access to places where they can speak and listen, and then, after reflection, speak and listen once more. A basic rule is that a street or a park is a quintessential forum for the exercise of First Amendment rights. See *Ward v. Rock Against Racism*, 491 U. S. 781, 796 (1989).

577. FB brags that it offers its users a free facility for communication of all kinds. See *Reno v. American Civil Liberties Union*, 521 U. S. 844, 868 (1997).

578. FB users can debate religion and politics with their friends and neighbors or share vacation photos. All fifty states, thousands of cities and towns, and almost every elected official have FB accounts.

579. The First Amendment of the U.S. Constitution and 42 U.S.C. § 1983 protects Zimmerman's freedom of speech and association and provide protection against political viewpoint discrimination in the unfettered access to and use of public spaces, quasi-public spaces, and limited public spaces, which includes the use of the FB platform.

580. The Fourth Amendment of the U.S. Constitution and 42 U.S.C. § 1983 protect Zimmerman's right to privacy. See *Puckingham v. North Carolina*

581. 42 U.S.C. § 1983 is enforceable against FB Defendants because FB provides to its users a public free speech forum of unequalled proportions and audience reach that make state fairs and parks seem negligible.



582. FB is also a quasi-state actor because it wields potent monopolistic and political powers and is currently getting ready to launch its own international currency.

583. The state constitutions of North Carolina and California also provide constitutional free speech and privacy protections equal to those provided by the U.S. Constitution.

584. FB Defendants are quasi-state actors because they regulate and control the FB platform that served Plaintiffs and at least a billion other FB users' as a public and private communications platform.

585. FB Defendants acted deceptively, willfully, recklessly and unlawfully, individually and in concert, directly and indirectly, and motivated by their greed and political ideologies, maliciously violated Zimmerman's constitutionally protected rights of free speech, free association and privacy as well as his right to participate in free and fair elections.

586. FB Defendants discriminated against Zimmerman by blocking his unfettered access to his FB accounts for no expressed substantive reason, thus unlawfully censoring Plaintiff's political messaging, disallowing Zimmerman's communications with his thousands of FB "Friends," thus denying Zimmerman his right to express and promote his political and non-political ideas and to otherwise advertise and market his political and non-political books and to his FB "Friends" and others.

587. FB has never expressed a compelling reason for its blocking of Zimmerman's use of his FB accounts that, before being blocked by FB, he used to communicate with his

thousands of FB “Friends” and to advertise his political viewpoints and political and non-political books and receive messages from his FB “Friends.”

588. FB conducted these unconstitutional activities after repeatedly bragging publicly and privately, that its foundational mission is to enable the citizens of this planet to freely communicate with one another.

589. Treasonous and unconstitutional conduct against the U.S. and its citizens shall consist not only in levying conventional war against them, or in adhering to their enemies, but also in providing them aid and comfort as FB did when they facilitated the Russian cyberattack on the 2016 U.S. presidential elections.

590. Chapter 18 of the U.S.C. sets out the punishment for treasonous conduct: “Whoever, owing allegiance to the United States, levies war against them or adheres to their enemies, giving them aid and comfort within the United States or elsewhere, is guilty of treason and shall suffer death, or shall be imprisoned not less than five years and fined under this title but not less than \$10,000; and shall be incapable of holding any public office in the United States.”

591. Although the *U.S. Constitution* defines treasonous conduct narrowly, in *United States v. Burr*, 159 U.S. 78 (1895), U.S. Supreme Court Chief Justice John Marshall in delivering the Court’s opinion regarded war as not an abstract term, and defined treasonous as an assemblage of people who intend to use actual force against the government, and/or adhering to enemies of the U.S. and/or by giving enemies of the U.S. aid and comfort.

592. Later, in *Cramer v. United States*, 325 U.S. 1 (1945) the U.S. Supreme Court made clear that the provision of "aid and comfort" has to consist of an affirmative act during war, such as the Russian launched cyberattack on the 2016 U.S. presidential election cycle as knowingly facilitated by FB and as described throughout this Complaint, which is the modern equivalent of conventional warfare.

593. Since at least 2014, Russian intelligence agents and operatives in concert with FB the Trump Campaign, Cambridge Analytica, Robert Mercer and others have been conducting malicious cyberwarfare against the U.S., and its citizens and still are.

594. That cyberwarfare shares the same ultimate objective as conventional warfare, namely, among other things, the destruction of our democracy and the rule of law.

595. As cyberwarfare is the functional equivalent of conventional warfare, the willful and reckless actions and inactions of FB Defendants in facilitating the cyberattacks on the 2016 U.S. presidential election cycle qualify as substantive, identifiable, treasonous actions because those actions "adhered to the enemy" by rendering Russia "aid and comfort," by willfully and for profit facilitating Russia's malicious cyberwarfare against the U.S. and the U.S. public, including Zimmerman.

596. Also, by failing to protect Zimmerman against and report the numerous willful invasions of Plaintiff's FB user' information, FB Defendants have violated Plaintiff's Fourth Amendment right to privacy.

597. The constitutions of California and North Carolina are also on point.

598. For example, California's *Constitution* at Article 1 *Declaration of Rights*: Section

1 establishes a citizen's privacy rights declaring: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." Section 28, deals with victim's rights.

599. North Carolina's *Constitution* Article 1, Section 10 establishes the right to free elections.

600. At a minimum, unconstitutional, other unlawful and possibly treasonous conduct of FB caused Zimmerman to suffer losses of his reasonable expectation to exercise his constitutional and other rights and privileges using the FB platform.

601. Zuckerberg has admitted he and others at FB were aware of the spread of Russian propaganda on the FB platform and did nothing to prevent it, instead pocketing Russian rubles and other currency from to sale of advertising space to Russian operatives.

602. Zimmerman had a reasonable expectation to use his FB accounts, which prior to having his accounts blocked by FB, to communicate with thousands of his FB "Friends" and to promote and advertise his political viewpoints and political and non-political books and receive messages and book orders from his FB "Friends."

603. FB Defendants willfully and recklessly enabled the unfettered access to Plaintiff's FB user information and that of their FB "Friends" without any authorization from Plaintiff by numerous third parties using various computer applications and telephonic devices.

604. A massive public outcry followed the revelation of FB's unconstitutional and

other tortious practices that eventually led to multiple ongoing foreign and domestic investigations of FB by governmental regulators and legislators and numerous private lawsuits

605. Further, the extent of the authorized and unauthorized FB user' information plundered by third parties from Plaintiffs will never be fully known and can continue far into the future.

606. Plaintiffs were substantially harmed and will continue to be harmed by the FB facilitated intrusion into Zimmerman's private affairs as detailed throughout this Complaint and FB Defendants active participation in the successful sabotage of the 2016 U.S. presidential elections that enabled the illegitimate and unlawful election of Trump.

607. Based on FB's intentionally deceptive, willful, reckless and unlawful actions and inactions as set out throughout this Complaint, Plaintiffs seek injunctive relief in the form of: (1) A FB-funded investigation to identify every third party that has had unfettered access to Plaintiff's FB user information, and how those third parties gained that access and how they used Plaintiff's FB user information and the destruction of it; (2) certification by FB that no third parties are currently able to access Plaintiff's FB user information from FB's information files and those of third parties that obtained it from FB; and (3) destruction by FB of all of Plaintiff's FB user information now in FB and third party information files.

608. The cyber-sabotage of elections by saboteurs deploying various cyberweapons is a relatively new phenomena and primarily engaged in by well-heeled organizations and

persons like, as here, the Trump Campaign, FB, Russian intelligence agents and operatives and right-wing billionaires like Robert Mercer seeking to enrich themselves, grow their political power, undermine free elections, democratic institutions and values and the rule of law.

609. In late May 2019, Monica Bickert, FB's V.P. Product Policy, publicly defended FB having allowed a doctored derogatory video of House Speaker Nancy Pelosi, to run on the FB platform, stating "FB will continue to host a video of Nancy Pelosi that has been edited to give the impression that the Democratic House speaker is drunk or unwell."

610. The Pelosi defamation facilitated by FB is but the latest incident highlighting FB's willful failures to deal with disinformation, misinformation, lies and hate speech.

611. Rudy Giuliani, the President's personal lawyer, was among the President's supporters who promoted the derogatory Pelosi video He tweeted a link to a copy of the video on FB stating: "What is wrong with Nancy Pelosi? Her speech pattern is bizarre."

612. One version of the doctored Pelosi video, which FB has allowed to continue running on a FB page is entitled "Politics WatchDog" and has been viewed millions of times, attracting comments speculating on Pelosi's health, supposed use of drugs, and other apparent ailments.

613. Despite the apparently malicious intent of the video's creator, FB has said it will only downgrade its visibility in users' newsfeeds and attach a link to a third party factchecking site pointing out that the clip is misleading.

614. As a result, although it is less likely to be seen by accident, the doctored video will continue to be seen.
615. FB was forced into taking this excruciating minimalist remedial action after the *Washington Post* reported the story.
616. The President tweeted a different altered video of Pelosi, which aired on a *Fox News* business broadcast, and had been heavily edited to make it appear as if she was stuttering and slurring her language. The President's tweet said: "PELOSI STAMMERS THROUGH NEWS CONFERENCE".
617. Alarming concerns have been raised about the enormous impact of the future use of disturbingly realistic fake or doctored videos by election riggers and other miscreants.
618. In addition to suffering the tortious and possibly treasonous conduct of FB Defendants, Zimmerman had a reasonable expectation of privacy when using FB to engage in online activity; and (2) a reasonable expectation that FB would not participate with Russian operatives the Trump Campaign, Robert Mercer and others in conduct that eventually led to the successful sabotage of the 2016 U.S. presidential elections.
619. Third parties tracked and extracted Plaintiff's FB user' information from FB's information repository, tracking and extracting that Plaintiffs did not authorize and by doing so willfully intruded into Zimmerman's solitude, seclusion and private affairs.
620. FB willfully designed its platform and established policies and procedures governing its use in such a way so as to readily enable the plundering, without any authorization by Plaintiffs of Plaintiff's FB user' information and that of their FB

“Friends” by third parties.

621. Numerous privacy intrusions by third parties were and are highly offensive to Plaintiffs and would be to any reasonable person or business. This is evidenced by the immense public outcry following the revelation of FB’s failure to protect the privacy of its users’ FB-stored information.

622. Further, the extent of the intrusions on Zimmerman’s right to privacy and the extent to which that plundered information was used and for what purposes will never be fully known because privacy intrusions and information plunders involve obtaining and sharing Plaintiffs FB user’ information and that of their FB user’ with potentially known unknown third parties for unknown purposes in perpetuity.

623. During the 2016 U.S. presidential elections a majority of Americans received more fake news and fake stories than factual news and stories broadcast over FB, FB-owned Instagram and FB-owned WhatsApp.

624. Of the twenty most shared fake news and stories broadcast over FB-owned platforms during the final phase of the 2016 U.S. presidential elections seventeen were either pro-Trump or anti-Clinton. See *How to Rig and Election*, chapter 4, by Nic Cheeseman and Brian Klaas.

625. As a direct and proximate result of the conduct of FB, Plaintiffs have sustained significant harm, entitling them to nominal and punitive damages in an amount to be established at trial.

626. Inasmuch as FB have amassed massive amounts of wealth, only a massive award



of punitive damages is likely to deter FB from engaging in future election sabotage and related unconstitutional and tortious conduct.

**COUNT FOUR– BREACH OF THE IMPLIED COVENENT OF GOOD FAITH AND FAIR DEALING**

627. Plaintiffs incorporate by reference all paragraphs contained throughout this

Complaint as though fully set forth herein.

628. Every contract imposes upon each party a duty of good faith and fair dealing in its performance and its enforcement.” See *Restatement (Second) of Contracts* § 205 (1981).

629. Plaintiffs were required by FB-constructed contracts to provide their personal and business information in order to register to use the FB platform and always used it responsibly.

630. Implicit and explicit in the contractual agreements between FB and Plaintiffs was FB’s obligation to protect the privacy of the Plaintiff’s FB user’ information.

631. Even if not explicitly stated, which it was, FB’s information privacy protection duty is read into contracts and functions as a supplement to the express contractual covenants in order to prevent a transgressing party from engaging in conduct which (while not technically transgressing the express covenants) frustrates the other party’s rights to the benefit of the contract.

632. Thus, any claim on the part of FB that technically it was permitted to allow the collection and transmittal of Plaintiff’s FB user’ information must be read in the context

of, and give way to, those user's rights to the benefit of the contract, including the terms strictly delimiting such activity.

633. The duty to perform contractual obligations in good faith applies to FB's agreements governing information collection, use, and protection, including its "Terms of Service," "Information Use Policy" and "Statement of Rights and Responsibilities."

634. In order not to frustrate the reasonable expectations of Plaintiffs under these sections and others in the FB-constructed contract and generally, FB was bound not to allow the access, collection, and transfer of Plaintiff's FB user' information to any third party.

635. But by failing to act reasonably in securing the privacy of Plaintiff's FB user' information, FB breached the covenant of good faith and fair dealing.

636. As a result of the aforesaid breach of the implied covenant of good faith and fair dealing, Plaintiffs have been harmed and have suffered damages by way of the widespread past and future dissemination of their FB user' information and that of their FB "Friends."

637. At a minimum, even if Plaintiffs had not suffered equitable or other damages nominal damages recoverable under Cal. Civ. Code § 3360.77.

**COUNT FIVE-INVASION OF PRIVACY–PUBLIC DISCLOSURE OF  
PRIVATE FACTS**

638. Plaintiffs incorporate by reference all paragraphs contained throughout this Complaint as though fully set forth herein.

639. Plaintiffs assert this Claim under California law

640. FB is a “person” within the meaning of the California Consumer Legal Remedies (“CLRA”) in that it is a corporation.

641. Plaintiffs are “consumers” within the meaning of CLRA in that they are individuals who seek or acquire services for personal, family, or business purposes.

642. CLRA § 1770(a)(5) prohibits “...representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have or that a person has a sponsorship, approval, status, affiliation, or connection which he or she does not have.”

643. CLRA § 1770(a)(14) prohibits “...representing that a transaction confers or involves rights, remedies, or obligations that it does not have or involve, or that are prohibited by law.”

644. . FB’s conduct as alleged herein violates CLRA’s ban of proscribed practices at Cal. Civ. Code (“CCC”) § 1770(a) subdivisions (5) and (14) in that, among other things, FB misrepresented its services by failing to disclose that it would and did allow access to its users’ information to its business partners, mobile carriers, software makers, security firms, banks, chip designers, device makers, retailers, wholesalers and numerous other third parties without FB user consent.

645. The FB user information privacy protection promises were false promises and entirely illusory.

646. With respect to “whitelisted” applications, FB collected revenue for the continued unfettered access to Plaintiffs’ information and did not disclose that it was doing so, nor did FB

offer to pay Plaintiffs for the use of their information by “whitelisted” applications, or any other third party or FB itself.

647. Plaintiffs have suffered injuries caused by FB’s misrepresentations and omissions because Plaintiffs suffered an invasion of their privacy as a result of FB exposing their information to its numerous third parties and were deprived of the income FB generated through its unauthorized use and sale of their information.

648. Plaintiffs seek equitable relief for FB’s violations of CLRA, including injunctive relief to enjoin the wrongful practices alleged herein, and to take corrective action to remedy past conduct, including ending all information-sharing partnerships still in effect and having FB direct all device makers, business partners, and “whitelisted” applications with Plaintiffs’ information stored in their information repositories to delete that information.

649. Sandberg, like Zuckerberg, has admitted FB’s numerous failures to protect the privacy of FB users’ information as well as Russia’s use of the FB platform to sabotage the US 2016 presidential election cycle.

650. Sandberg said: “There are things that we missed. We wish we had understood the Russian interference in the US election. We didn’t. We missed it.”

651. Sandberg avoided answering more pressing questions over the distribution of FB users’ private information.

652. Recently, an investigative reporters revealed that FB had ignored the privacy concerns of its users in a series of 2012 emails despite signing a “Consent Decree” with the FTC that mandated that FB fix their numerous failures to protect the privacy of their users’ information.

653. When asked by Caroline Hyde, a business news anchor on Bloomberg TV, to address its users privacy concerns of its users, Sandberg said: “I think there has been a growing understanding of how important privacy is and how we have to protect it.” I think if you look at some of the early iterations of the FB platform, we were allowing people to share too much information early on before 2014. If I used an app, I would share my information and my friend’s information. It’s really hard to remember — this is not an excuse because I think we should have done better, the real concern then, was we were hoarding information and not sharing it. People were very concerned that we were a walled garden.”

654. Sandberg explained that through trial and error FB realized it needed to share the “minimum amount of information.”

655. Sandberg compared FB to any new technology, from the printing press to radio or TV stating that: “There is some commonality to this experience. A new technology comes out. People celebrate it to see all the good it does, almost to the exclusion of any bad, then something bad happens, and people see that the bad can happen and they focus on that. That’s where the new rules are written,” she said. “New rules need to be written for the Internet and we want to be part of that.”

656. Later, Sandberg deflected a question on the call of FB co-founder Chris Hughes for the breaking up of FB stating: “When you think about what’s underlying this conversation is that people are worried about the size and power of US tech companies whether it’s ours or others. We understand that ... we have a big impact in the world.”

she said before turning to what she called a bigger threat. “People aren’t appropriately worried about Chinese companies, some of which are far bigger and have far many more people and services than we do, and I think that’s something that needs to be taken into account.”

657. Hyde wrapped up the interview asking Sandberg if she ever questioned her role as a leader given the onslaught of company disasters.

658. “Of course. I don’t know any good leaders that didn’t,” Sandberg said. “When we missed what happened with the Russian election, when we failed to respond quickly enough to Cambridge Analytica, of course.”

#### COUNT SIX-CIVIL CONVERSION

659. Plaintiffs incorporate by reference all paragraphs contained throughout this Complaint as though fully set forth herein.

660. Civil conversion is the wrongful exercise of dominion over the property of another. Here, FB Defendants exercised dominion over Plaintiff’s FB user’ information.

661. The elements of a claim for civil conversion are: (1) the plaintiff’s ownership or right to possession of the property unlawfully converted by defendants; (2) the defendant’s conversion by a wrongful act or disposition of property rights; and (3) damages.” See *Lee v. Hanley* (2015) Cal.4th 1225, 1240 [191 Cal.Rptr.3d 536, 354 P.3d 334].

662. Here, the Plaintiff’s right of ownership is undisputable. Here, FB Defendants have repeatedly admitted their wrongful and willful and reckless exercise of dominion over

Plaintiff's property, namely their FB user information, and disposed of it in numerous and various ways, and Plaintiffs are seeking appropriate damages.

663. It is not necessary that there be a manual taking of the property; it is only necessary to show an assumption of control or ownership over the property, or that the alleged converter has applied the property to his own use. See *Shopoff & Cavallo LLP v. Hyon* (2008) 167 Cal.App.4th 1489, 1507 [85 Cal.Rptr.3d 268].
664. Any act of dominion wrongfully exerted over the personal property of another inconsistent with the owner's rights thereto constitutes conversion. See *Plummer v. Day/Eisenberg, LLP* (2010) 184 Cal.App.4th 38, 50 [108 Cal.Rptr.3d 455].
665. Conversion is a strict liability tort. The foundation of the action rests neither in the knowledge nor the intent of the defendant. Instead, the tort consists in the breach of an absolute duty; the act of conversion itself is tortious.
666. Therefore, questions of the defendant's good faith, lack of knowledge, and motive are immaterial." See *Los Angeles Federal Credit Union v. Madatyan* (2012), 209 Cal.App.4th 1383, 1387 [147 Cal.Rptr.3d 768].
667. "The rule of strict liability applies equally to purchasers of converted goods, or more generally to purchasers from sellers who lack the power to transfer ownership of the goods sold. That is, there is no general exception for bona fide purchasers." See *Regent Alliance Ltd.*, 231 Cal.App.4th at p. 1181.

668. As the result of FB Defendants willful and reckless unlawful conversion activities, FB Defendants have willfully and recklessly interfered with Plaintiff's right of possession and control of their FB user' information.

669. As a direct and proximate result of FB's willfully unlawful conduct, Plaintiffs suffered injury, damage, loss and other harms and therefore seek compensatory damages in an amount to be established at trial.

670. As a direct and proximate result of the conduct of FB in converting Plaintiff's FB user' information, FB Defendants have acted with malice, oppression and in conscious disregard of the Plaintiff's privacy rights and Plaintiffs, therefore, seek an award of punitive damages in an amount to be established at trial.

#### **COUNT SEVEN-NEGLIGENCE AND GROSS NEGLIGENCE**

671. Plaintiffs incorporate by reference all paragraphs contained throughout this Complaint as though fully set forth herein.

672. FBs owed a duty to Plaintiffs to exercise reasonable care in the obtaining, using, and protecting of their FB user' information, arising from the sensitivity of their information and the expectation that their information was not going to be shared with third parties without their consent.

673. This duty included FB ensuring that no application developers, device makers or other third parties were collecting, storing, obtaining and/or selling Plaintiffs' FB user' information.

674. Plaintiffs' willingness to entrust FB with their information was predicated on the



understanding that FB would take appropriate measures to protect it.

675. FB had a special relationship with Plaintiffs as a result of being entrusted with their information, which provided an independent special duty of care.

676. FB knew that the information of Plaintiffs had value because there is an active market for FB user' information. Indeed, FB has received tens of billions of dollars from selling targeted advertising on its platform.

677. There is also an active black market for FB user' information.

678. FB received multiple warnings that its user' information was at risk.

679. In 2012, Sandy Parakilas, former FB operations manager warned FB's executives about the risks of application developers gaining unfettered access to FB information without their consent.

680. According to Parakilas, FB was not conducting regular audits of application developers use of the FB's platform.

681. FB ignored Parakilas's warning.

682. In 2012, FB executed a "Consent Decree" with the FTC agreeing to, among other things, clearly and prominently disclose its sharing of FB user' information with third parties.

683. Even so, FB continued to let application developers access its users' information without their consent.

684. And, as late as 2017, Alex Stamos, FB's then Chief of Security, warned FB executives about security risks on the platform in a written report concerning the circumstances leading to Cambridge Analytica obtaining FB users'

personal information.

685. Despite these and other numerous warnings, FB failed to take reasonable steps to prevent harm to Plaintiffs and its other users.

686. On April 30, 2014, FB announced a new “anonymous login” feature that would have allowed users to use an application without sharing any personal information. Yet, FB never implemented this feature.

687. On April 30, 2014, FB also announced a new “controlled login” feature to allow users to choose what information they shared with application developers before login in, but FB did not implement this feature until May 2015.

688. As early as December 11, 2015, FB received notice that application developer Aleksandr Kogan had sold FB user’ personal information to Cambridge Analytica; but FB waited until April 2018, more than three years later, to notify users that their personal information had been unlawfully misappropriated.

689. FB owed a duty to timely disclose to Plaintiffs that FB had allowed their information to be accessed by Cambridge Analytica and numerous other third parties.

690. Plaintiffs had a reasonable expectation that FB would inform them of the improper disclosure of their information.

691. FB breached its duties by, among other things: (a) failing to ensure that application developers, “whitelisted” applications, device makers and other third parties were not improperly collecting, storing, obtaining and/or selling Plaintiffs’ information without their informed consent; and (b) failing to provide adequate and timely notice that Plaintiff’s FB-stored content and information had been improperly obtained by Cambridge Analytica and

numerous third parties.

692. But for FB's breach of its duties, including its duty to use reasonable care to protect and secure Plaintiff's information, Plaintiff's information would not have been disclosed without their consent to third parties, which resulted in further misuse of Plaintiff's information.

693. Plaintiffs were foreseeable victims of FB's breach of its duties.

694. FB knew or should have known that allowing third parties to access Plaintiff's information would cause damage to Plaintiffs.

695. Public policy voids any waiver of liability that FB Defendants may raise.

696. The contracts between FB and Plaintiffs are of a type suitable for public regulation.

697. Indeed, FB is subject to public regulation due to its ubiquity and use by over a hundred million of Americans.

698. Using FB is often a matter of practical necessity for the many persons and businesses who are now addicted to use FB to coordinate daily activities, network, engage in political and cultural discourse and pursue interests and hobbies. To do these things, FB users must share their personal information with their FB "Friends."

699. FB maintains it is a free provider of communication services that wants to connect every person on planet Earth

700. Because of its enormous financial resources and monopolistic power, FB possesses a decisive advantage when dealing with any member of the public that seeks to use its

services, making any purported waiver of liability by FB unconscionable and unlawful.

701. The confidentiality of Plaintiff's FB user' information was and still is totally under FB's control.

702. FB violated its very own privacy protection promises by allowing numerous third parties to access Plaintiff's user' information.

703. Beyond mere negligence, FB's conduct also constitutes gross negligence due to FB's willful and reckless departure from ordinary standards of care and its knowledge that it had failed to secure the information of Plaintiffs and did nothing about it, including failing to notify Plaintiffs of its information privacy protection failures and doing nothing to correct those failures and even denying that the failures occurred.

704. As a result of FB's failure to safeguard Plaintiffs' user' information, Plaintiffs have suffered injury, which includes but is not limited to impermissible disclosure of their information, both directly and indirectly by FB, and exposure to a heightened, imminent risk of misuse, fraud, identity theft, voter fraud, medical fraud, and financial and other harms.

705. The information shared by FB with third parties allows this information to be aggregated with other information and allows third parties to identify and target Plaintiffs.

706. The injury to Plaintiffs was a proximate and reasonably foreseeable result of FB's breaches of its contractual duties and promises to Plaintiffs.

707. As a proximate result of FB's information privacy protection failures, Plaintiffs suffered damages in an amount to be established at trial.

**COUNT EIGHT-NEGLIGENT AND/OR FRAUDULENT MISREPRESENTATION**

708. Plaintiffs incorporate by reference all paragraphs of this Complaint as though fully set forth herein.

709. Plaintiffs suffered injury in fact and lost money or property as the proximate result of FB's negligent and/or fraudulent misrepresentations.

710. The FB user's information of Plaintiffs was taken by third parties who will and did use it for their own advantage.

711. Plaintiffs justifiably relied on the representations FB made in its publicly available privacy policy and elsewhere that it would not "share information we receive about you with others unless we have: received your permission [and] given you notice."

712. FB knew the falsity of its privacy protection representations, and they were made with the intent to deceive Plaintiffs into supplying FB with private confidential personal information.

713. FB's representations regarding the maintenance of user confidentiality and privacy were material to Plaintiffs' decision to provide FB with the personal information FB subsequently disclosed to numerous third parties.

714. Plaintiffs justifiably relied upon the representations of FB.

715. Plaintiffs suffered harm as a proximate result of FB's fraudulent acts.

716. As a direct and indirect result of FB's negligent and/or fraudulent misrepresentations, Plaintiffs are entitled to general, special punitive damages, reasonable

attorneys' fees if any, and costs, and any other relief in an amount to be established at trial.

### **COUNT NINE BREACH OF CONTRACT**

717. Plaintiffs incorporate by reference all paragraphs contained throughout this Complaint as though fully set forth herein.

718. At all relevant times, FB and Plaintiffs mutually assented to, and were bound by the version of FB's "Statement of Rights and Responsibilities" or later, the "Terms of Service," that was operative at the time each of the Plaintiffs registered to use the FB platform.

719. At all relevant times, FB affirmed that FB would "not share your information with advertisers without your consent." None of FB contracts informed and obtained users' meaningful and lawfully obtained consent to share their information with advertisers and other third parties, or disclosed that such information would be shared if FB users' "Friends" entered into an agreement which permitted third parties to collect their FB "Friends" information.

720. Thus, the FB non-negotiable, non-negotiable contracts did not authorize FB to share Plaintiffs' user' information with FB's business partners or mobile carriers, software makers, security firms, banks, credit reporting and government agencies, chip designers, device makers, retailers, wholesalers or any other third party.

721. The FB contracts with Plaintiffs also did not authorize FB to make the information that users shared with "Friends" available to any third party.

722. Contrary to the FB contracts with Plaintiffs, FB knowingly allowed numerous third parties who made their applications available through Graph API v1.0 to sell the information regarding Plaintiffs that they had collected via applications that used the FB platform.

723. The FB contracts required FB to protect the information of its users.

724. The FB contracts affirm that users' information would not be shared with advertisers or any other third party without their affirmative consent.

725. Likewise, these same FB "Terms of Service" informed users that their privacy setting would control who had access to their content and information, but this was untrue. FB did not disclose that users were required to affirmatively "opt out" of sharing their information with third parties in the FB contracts.

726. As set forth herein, Plaintiffs' information is of considerable value as demonstrated by FB's calculation of the Average Revenue Per User that FB calculates.

727. There is an active market for the information generated by FB users, both individually and especially in the aggregate. FB generates billions of dollars in revenues through targeted advertising delivered to third parties, curated through the collection and aggregation of FB's user information.

728. There is also an active black market for user information.

729. The remedy for the FB breaches of the FB contracts is what FB gained through their breaches.

730. The value of the information accumulated by FB about a user increases with the amount of information FB collects. Thus, over time, FB's benefit of the bargain has multiplied dramatically.

731. . As a result of the breach, Plaintiffs have been harmed and have suffered damages by losing the value of their information.

#### **COUNT TEN-WILLFUL INFLICTION OF EMOTIONAL DISTRESS**

732. Plaintiffs incorporate by reference all paragraphs contained throughout this Complaint as though fully set forth herein.

733. FB knew and were plainly indifferent to the fact that their blocking of Plaintiff's FB personal and business accounts would cause Zimmerman severe emotional distress.

734. FB knew that their failure to protect Plaintiff's user' information from access by third parties not authorized for such access by him would cause Zimmerman severe emotional distress.

735. FB knew that Plaintiff's plundered FB user' information was not intended for use in sabotaging the 2016 U.S. presidential elections or other U.S. elections and such use would cause Zimmerman severe emotional distress.

736. The willful unlawful conduct of FB as set out in this Complaint was extreme, outrageous, and beyond the bounds of decency.



737. As a direct and proximate result of the conduct of FB, Zimmerman has suffered severe or extreme emotional distress, entitling him to recover damages in an amount to be established at trial.

738. The outrageous, malicious, and willful misconduct of FB conspiring with a hostile foreign governments and others to use Plaintiff's plundered FB user' information to influence the 2016 U.S. presidential elections and other purposes entitles Plaintiffs to receive punitive damages so as to deter FB from repeating such outrageous conduct in the future.

#### **COUNT ELEVEN-COMMON LAW CIVIL CONSPIRACY**

739. Plaintiffs incorporate by reference all paragraphs contained throughout this Complaint as though fully set forth herein.

740. "The basis of a civil conspiracy is the formation of a group of two or more persons who have agreed to a common plan or design to commit a tortious act.' The conspiring FBs must also have actual knowledge that a tort is planned and concur in the tortious scheme with knowledge of its unlawful purpose." See *Kidron v. Movie Acquisition Corp.*, 40 Cal.App.4th 1571, 1582 (1995). A conspiracy may be inferred from circumstances, including the nature of the acts done, the relationships between the parties, and the interests of the alleged co-conspirators.

741. Well before information repositories, FB knew and have admitted that they knew that FB was deliberately and for its own profit and other purposes allowing third parties to access and collect Plaintiff's user' information without his consent and that FB's

information security measures were so grossly inadequate that malevolent third parties could also access and collect Plaintiff's user' information. Nevertheless, FB continued to recklessly ignore FB's gigantic information security problem and instead did little to nothing to protect Plaintiff's FB user' information or even bother to warn them about the security problems and, instead, openly lied to Congress and foreign governments that FB was dedicated to the highest and most advance security practices and protocols.

742. FB willfully opted to not disclose to Plaintiffs that their FB accounts and associated user information are an easy target for information plunderers and that FB was not implementing measures to protect them.

743. FB conspired among themselves and with others, including the Trump Campaign, Robert Mercer and Russian officials, agents and operatives to act in concert for unlawful purposes by unlawful means as described in detail throughout this Complaint and have admitted as much. See Section X and the entirety contained throughout this Complaint.

744. In particular, FB and their co-conspirators agreed to publicly disclose on the Internet and elsewhere Plaintiff's FB user' information and that of their FB "Friends" that were plundered from FB by Cambridge Analytica, a now bankrupt business entity funded, directed and controlled by Mercer and deliberately allowed third parties to access and collect Plaintiff's FB user' information without Plaintiff's consent or knowledge.

745. FB conspiratorial conduct violated California civil conspiracy law that maintains that a conspiracy is an agreement by two or more persons, Mark Zuckerberg, Sheryl Sandberg and other FB executives to commit a wrongful act.

746. Such an agreement may be made orally or in writing or may be implied by the conduct of the parties. A conspiracy may be inferred from circumstances, including the nature of the acts done, the relationships between the parties, and the interests of the alleged co-conspirators. “While criminal conspiracies involve distinct substantive wrongs, civil conspiracies do not involve separate torts. The doctrine provides a remedial measure for affixing liability to all persons who have ‘agreed to a common design to commit a wrong.’” See *Choate v. County of Orange* (2000) 86 Cal.App.4th 312, 333 [103 Cal.Rptr.2d 339].

747. “As long as two or more persons agree to perform a wrongful act, the law places civil liability for the resulting damages on all of them, regardless of whether they actually commit the tort themselves. ‘The effect of charging . . . conspiratorial conduct is to implicate all . . . who agree to the plan to commit the wrong as well as those who actually carry it out.’” See *Wyatt v. Union Mortgage Co.* (1979) 24 Cal.3d 773, 784 [157 Cal. Rptr. 392, 598 P.2d 45].

748. “Conspiracy is not a cause of action, but a legal doctrine that imposes liability on persons who, although not actually committing a tort themselves, share with the immediate tortfeasors a common plan or design in its perpetration.

749. By participation in a civil conspiracy, a co-conspirator effectively adopts as his or her own the torts of other co-conspirators within the ambit of the conspiracy. In this way, a co-conspirator incurs tort liability co-equal with the immediate tortfeasors.” See *Applied Equipment Corp. v. Litton Saudi Arabia Ltd.* (1994) 7 Cal.4th 503, 510–511 [28 Cal.Rptr.2d 475, 869 P.2d 454]

750. As a direct and proximate result of the overt and covert acts of FB, Plaintiffs have sustained significant harm, entitling them to recover damages in an amount to established at trial.

**COUNT TWELVE-DECEIT BY CONCEALMENT OR OMISSION**

751. Plaintiffs incorporate by reference all paragraphs contained throughout this Complaint as though fully set forth herein.

752. Under California law, a plaintiff may assert a claim for deceit by concealment based on “[t]he suppression of a fact, by one who is bound to disclose it, or who gives information of other facts which are likely to mislead for want of communication of that fact.” CCC § 1710(3).

753. These following actions are “deceit” under CCC § 1710 because FB suppressed facts that they were duty-bound to disclose, especially given FB’s assertions about protecting the privacy of Plaintiffs. FB has committed deceit by concealment in three distinct ways.

754. FB did not disclose known risks that third party application developers would sell or disperse user information. FB received multiple warnings that Plaintiffs’ information was at risk.

755. In 2012, Sandy Parakilas, former FB operations manager, warned FB’s executives about the risks of application developers gaining unfettered access to users’ personal information without their consent on FB’s platform. Yet, FB ignored Parakilas’s warnings.

756. In October 2012, FB reached a settlement with the FTC agreeing to clearly and prominently disclose its sharing of information with third parties; yet, FB continued to let application developers access users' information without their consent.

757. As late as 2017, Alex Stamos, FB's former Chief of Security, warned FB executives about security risks on the platform. In an internal meeting held in 2017, Stamos warned of "willful decisions to give unfettered access to information and systems to engineers to make them 'move fast' but that creates other issues for us."

758. In 2017, Stamos states that he provided a written report concerning the circumstances leading to Cambridge Analytica obtaining users' personal information. FB edited and published a whitewashed version of this report concealing any wrongdoing.

759. FB did not audit what happened to information that was provided to third parties because it knew it would find abuse. FB did not disclose to Plaintiffs the risks that they faced from these warnings and did not inform Plaintiffs that their information was insecure once it was shared with application developers or other third parties.

760. FB knew that Plaintiffs' information was not secure. Even so, FB ignored the warnings above that audits were necessary to secure Plaintiffs' information because FBs did not know what third parties were doing with it after it left FB's servers.

761. FB willfully, deceptively and recklessly failed to secure Plaintiffs' FB user' information and content because they wanted to encourage application developers, FB business partners and numerous other third parties to exploit that information and content. FBs knew that appropriate security measures, such as audits, would discourage third

parties. FBs did not engage in such audits or conduct other reasonable efforts to protect Plaintiffs' information.

762. FB had a duty to inform Plaintiffs that FB had become aware that they had failed to secure their information. FB knew in 2015 that it had failed to secure Plaintiffs' information, including by making it available to numerous third parties.

763. FB willfully concealed that Plaintiffs' FB user information and content was insecure because they wanted Plaintiffs to continue to generate content for their business partners.

764. FB failed to disclose the risks Plaintiffs faced with the intention to deceive them about the security of their information.

765. FB failed to disclose to Plaintiffs that it had failed to secure information for dozens of other third party Applications, even after they became aware of the Cambridge Analytica unlawful misappropriation of FB user' information from tens-of-millions of FB users and failed to conduct any investigation into the extent or use of the FB user' information to which it until March of 2018.

766. Plaintiffs been aware that FB had failed to implement adequate security measures, they would not have shared their information and content with FB to the extent that they did, if at all.

767. Plaintiffs were damaged because, as a result of FBs' deceit, their content and information have been disclosed to third parties without their consent.

768. Plaintiffs were also damaged because, as a result of FBs' deceit, their privacy was invaded.

769. Plaintiffs are at heightened risk of identity theft, phishing schemes, and other malicious attacks. Due to FB's deceit, Plaintiffs' information and content were compromised, and may be available on the dark web or in the hands of foreign nationals.

770. Plaintiffs are therefore entitled to "any damage" that they have suffered under CCC Section 1709.

771. FB have also committed deceit by failing to meaningfully disclose to Plaintiffs how FB allows other third parties, including but not limited to application developers, "whitelisted" applications, device makers, mobile carriers, software makers, and others to obtain their FB user' information notwithstanding their privacy settings.

772. With respect to "whitelisted" applications, FB failed to disclose that FB would provide the applications with FB users' information as long as the "whitelisted" applications provided FB with revenues that were based on how many FB users' information they accessed.

773. FB failed to disclose that these FB users and their "Friends" could not control "whitelisted" applications' access with their privacy settings.

774. FB allowed "whitelisted" applications to continue to receive information from users and their "Friends" notwithstanding users' privacy settings.

775. FB stripped privacy settings from photos and videos that had been designated private, in violation of its own privacy policies. As a result, those applications could not honor users' privacy settings.

776. In addition, computer applications were able to circumvent FB user's privacy of platform settings and access FB "Friend's" information, even when the FB user disabled the FB Platform.

777. FB misled users to believe that they were protecting users' privacy and failed to disclose that they were sharing users' information with third parties.

778. FB did not disclose that, notwithstanding privacy settings that purported to provide Plaintiffs with control over their information, FB allowed third -parties to harvest and store personal information.

779. FB had a duty to provide accurate information to Plaintiffs about how their information was disclosed to third parties by FB. FBs knew that Plaintiffs shared personal and sometimes intimate details about their lives, personalities, and identities.

780. FB encouraged Plaintiffs to share information by assuring them that FB would respect their choices concerning privacy.

781. FB willfully concealed and omitted material information regarding how FB disclosed Plaintiffs' information in an effort to create a false sense of security and privacy for Plaintiffs.

782. FB did this because they wanted Plaintiffs to provide more detailed information, whose value would be increased by that additional detail. Third parties would thereby pay a higher price for unfettered access to that information, increasing FB's revenue.



783. Had Plaintiffs been aware of the full extent of how FB collected and used their information, they would not have shared their information on their devices on the FB platform to the same degree that they did, if at all.
784. Plaintiffs were damaged because their information was disclosed to third party device makers and others without their consent.
785. As a result of the disclosures of Plaintiffs' FB user' information to these third parties, Plaintiffs could not take remedial measures to protect themselves from identity theft, scams, phishing, unwanted political targeting, even surveillance and other forms of harassment.
786. Moreover, Plaintiffs would have behaved differently and shared less information had these acts been disclosed.
787. FB deliberately withheld notice because it did not want to discourage user sharing and engagement on its platform.
788. FB also failed to disclose to Plaintiffs how their Fb user' information was being collected, shared and aggregated to develop digital profiles or dossiers of each FB user.
789. Those dossiers comprised of FB user information were combined with other sources to de-anonymize this information such that FB users could be individual targeted.
790. FB had a duty to disclose the full extent to which it allowed Plaintiffs to be targeted by advertisers and marketers because it promised in its Contracts that it would not share users' information with advertisers without their consent. FBs' duty also arose from its affirmative representations that (1) Plaintiffs could control their information, and (2) third parties could not access personal information absent users' consent.

791. FB knew that advertisers were targeting Plaintiffs with messages based upon FB derived information, combined with information derived from other information brokers.
792. FB was the vehicle to target Plaintiffs by drawing upon the vast amounts of content information collected by FB and matched with additional information collected about them by third party information brokers.
793. FB knew that psychographic marketing and other targeted advertising was lucrative, and that advertisers paid a premium to combine FB user' information with information from third party information brokers.
794. FB did not disclose to Plaintiffs that advertisers were combining information from information brokers with FB-derived information to target them with advertisements and psychographic marketing, as well as building digital dossiers.
795. FB intended to deceive Plaintiffs about their vulnerability to targeted advertisements and about the degree to which sharing their FB user' information and content on FB directly led to targeted messaging.
796. Had Plaintiffs known the extent to which FB shared their information with third parties, and how it was aggregated and made available to advertisers and political operatives and others, Plaintiffs would have not shared their information and content on FB to the extent that they did, if it all.
797. Plaintiffs suffered injury as a direct result of FB' deceit.

798. Plaintiffs FB user' information and content were used and aggregated by advertisers and other third parties without their consent, and for nefarious purposes and in return FB received substantial advertising revenues.

799. Had Plaintiffs known the extent and degree to which their FB user' information was provided to third parties Plaintiffs would have required compensation for this use of their FB user information.

800. Plaintiffs suffered economic injury as a result of FB's fraud. Plaintiffs have an economic and privacy interest in their FB user' information, which has value beyond the FB platform.

801. FB knew that Plaintiff's FB user' information was worth at least \$0.10 for each application to view a FB user's profile, and FB orchestrated its "whitelisting" to require applications to pay to FB revenues that were equivalent to the number of Fb users and their "Friends" that each application had.

802. As a result, FB have been unjustly enriched by its deceit, and Plaintiffs are entitled to restitution.

803. Restitution is a remedy that may be awarded to prevent unjust enrichment when the FB has obtained some benefit from Plaintiffs through fraud, duress, conversion or similar misconduct. See *McBride v. Boughton*, 123 Cal.App.4th 379, 387-388 (2004).

804. For all types of fraudulent omissions complained of here, Plaintiffs s seek disgorgement of FB's profits that were made with the use of Plaintiff's FB user' information.

805. Disgorgement is appropriate because FB profited from Plaintiffs' content and information wrongfully obtained by generating revenues from third party computer application developers and advertisers.
806. Disgorgement is necessary in order to deter future unauthorized use of Plaintiff's FB user' information. Disgorgement is also necessary to the extent that the value of Plaintiff's user' information cannot be assessed by ordinary tort damages. Public policy supports the use of disgorgement here to disincentivize the type of deception that FB used in exploiting Plaintiff's FB user information.
807. In the future, as a direct result of FB's unlawful conduct Plaintiffs may also suffer further damages of a nature that are purely speculative at this time.
808. Accordingly, as a result of the misconduct of FB, Plaintiffs are entitled to recover damages, including punitive damages under CCC § 3294(a) in an amount to be established at trial.

### **COUNT THIRTEEN-FRAUD**

809. Plaintiffs incorporate by reference all paragraphs contained throughout this Complaint as though fully set forth herein.
810. FB deceit as alleged herein is fraud under CCC § 3294(c)(3) in that it was deceit or concealment of a material fact known to the FB and FB willfully deprived Plaintiffs of legal rights and otherwise caused injury to them.
811. "The elements of fraud that will give rise to a tort action for deceit are: "(a)



misrepresentation (false representation, concealment, or nondisclosure); (b) knowledge of falsity (or ‘scienter’); (c) intent to defraud, i.e., to induce reliance; (d) justifiable reliance; and (e) resulting damage.’ ” See *Engalla v. Permanente Medical Group, Inc.* (1997) 15 Cal.4th 951, 974 [64 Cal.Rptr.2d 843, 938 P.2d 903]; *Medallion, Inc. v. Clorox Co.* (1996) 44 Cal.App.4th 1807, 1816 [52 Cal.Rptr.2d 650] [combining misrepresentation and scienter as a single element].

812. “Fraud is a willful tort; it is the element of fraudulent intent, or intent to deceive, that distinguishes it from actionable negligent misrepresentation and from nonactionable innocent misrepresentation.

813. It is the element of intent which makes fraud actionable, irrespective of any contractual or fiduciary duty one party might owe to the other.” See *City of Atascadero v. Merrill Lynch, Pierce, Fenner & Smith* (1998) 68 Cal.App.4th 445, 482 [80 Cal.Rptr.2d 329]. Fraudulent intent is an issue for the trier of fact to decide.” See *Beckwith v. Dahl*, (2012) 205 Cal.App.4th 1039, 1061.

814. As a direct and proximate result of the overt and covert acts of FB as alleged throughout this Complaint, Plaintiffs have sustained significant harm, entitling them to recover damages in an amount to established at trial.

#### **COUNT FOURTEEN- WILLFUL MISREPRESENTATION**

815. Plaintiffs incorporate by reference all paragraphs contained throughout this Complaint as though fully set forth herein.

816. Plaintiffs claim that FB willfully and for profit and other purposes made at least one important false representation that substantially harmed Plaintiffs, that being that they would protect the privacy of Plaintiff’s FB user’ information.

817. When the FB made that false representation, they knew it was false and misleading and made it with a conscious and reckless disregard for the truth.
818. FB intended that Plaintiffs rely on their misrepresentation.
819. Zimmerman did reasonably rely on FB's misrepresentation.
820. Plaintiffs were harmed and Plaintiff Zimmerman's reliance on FB's representation was a substantial factor in causing that harm.
821. These willful misrepresentations by FB constitute "deceit" under CCC § 1710 in that it is suppression of a fact by one who is bound to disclose it, or who gives information of other facts which are likely to mislead for want of communication of that fact.
822. As a result of this deceitful misrepresentation by FB the user's information of Plaintiffs was compromised, placing Plaintiffs at a great risk of identity theft and other crimes.
823. As a result of FB's deceitful misrepresentations, FB Defendants are liable under CCC § 1709 for the damage their conduct inflicted on Plaintiffs.
824. Plaintiffs also suffered diminution in value of their information in that it may now or in the future be readily available to plunderers on the "Dark Web" and elsewhere.
825. Plaintiffs may also suffer consequential out of pocket losses for procuring credit freeze or protection services.

826. As a result of the conduct of FB Defendants, Plaintiffs are entitled to recover damages, including punitive damages under CCC § 3294(a) in an amount to be established at trial.

**COUNT FIFTEEN-CIVIL RICO CONSPIRACY**

827. Plaintiffs incorporate by reference all paragraphs contained throughout this Complaint as though fully set forth herein.

828. Plaintiffs assert FB Defendants' violations of 18 U.S.C. § 1962(C) and the Enterprise constitutes a RICO Enterprise pursuant to 18 U.S.C. § 1961(4).

829. The RICO Enterprise and/or the RICO Association-in-Fact Enterprise ("Enterprise") has been operating since at least 2014 and at various times was and for the most part still is composed of FB Defendants, Russian officials, intelligence agents and operatives, the Trump Campaign, Aleksandr Kogan, Robert Mercer, Jared Kushner, Cambridge Analytica, Stephen Bannon and numerous other persons and entities.

830. The Enterprise engaged in, and still engages in, activities that affect interstate commerce.

831. The Enterprise was formed for the purpose of using unlawfully obtained FB user' information and other unlawfully obtained information for the targeted transmission to prospective voters of political propaganda, misinformation, disinformation, misleading political advertising and other messaging.to, as matters turned out, successfully help sabotage the 2016 U.S. election cycle.

832. Aleksandr Kogan participated in the Enterprise by (i) creating a U.K. company that was part of a scheme to dupe FB users' into providing their FB user' information to



to the U.K. company, which was part of a broader scheme to unlawfully plunder the FB user' information of tens-of-millions of FB users.

833. Bannon participated in the Enterprise by, among other things: (i) helping to found Cambridge Analytica by obtaining funding for Cambridge Analytica from Robert Mercer (a U.S. citizen); (ii) acting as a vice-president of Cambridge Analytica; (iii) helping to supervise the activities of Cambridge Analytica; and (iv) serving as a senior political advisor to the Trump Campaign and the Trump administration.

834. These actions were undertaken with fraud, malice and a willful conscious disregard of the rights or safety of Plaintiffs and the majority of Americans who voted in the 2016 presidential election cycle. .

835. FB Defendants agreed to and did conduct and participate, directly and indirectly, in the conduct of the Enterprise's affairs in a pattern of racketeering activity.

836. Prior to and concurrent with its participation in the Enterprise, FB willfully and recklessly devised a scheme with artifice to defraud FB users and to obtain, sell, trade and use FB user's information by false pretenses and representations, including, but not limited to, the representation that the information would only be used for academic purposes.

837. The payments made to takers of the "This is Your Digital Life" quiz were in furtherance of the fraudulent scheme and were made by wire transfer or other electronic means through interstate or foreign commerce.

838. The acts of wire fraud averred herein also constitute a pattern of racketeering activity pursuant to 18 U.S.C. § 1961(5).
839. FB aided and abetted the co-conspirators by misleading its users to believe that their FB us' information was safe, while allowing numerous third parties to access and use the information of non-consenting FB users without their permission and knowledge.
840. FB directly participated in the conspiracy by misleading quiz-takers that they were allowing third parties unfettered access to only their information for academic purposes only, when in fact they were allowing unfettered access to their FB "Friends" information, and by fraudulently obtaining the information, selling it and trading it in interstate and foreign commerce, and using it to sabotage elections.
841. Plaintiffs were harmed by FB conduct because the private information they did not intend to become public or disclose to third parties was acquired by persons and entities who used it to unlawfully sabotage elections and other nefarious purposes.
842. Furthermore, the security breach put Plaintiffs are in imminent and real danger of having their identities stolen by anyone willing to pay these unscrupulous companies for their FB user' information.
843. In addition, Plaintiffs spent considerable time and money unsuccessfully attempting protect against the misuse of their plundered FB user information.
844. As a direct and proximate FB Defendants racketeering activities and violations of 18 U.S.C. § 1962(c), Plaintiffs have been injured and request judgment in their favor and against FB Defendants for compensatory, treble and/or punitive damages with interest,

the costs of suit and attorneys' fees, if any, , and other and further relief as this Court deems just and proper.

**COUNT SIXTEEN-VIOLATION OF THE STORED COMMUNICATIONS ACT**

845. Plaintiffs incorporate by reference all paragraphs contained throughout this Complaint as though fully set forth herein.

846. The Stored Communications Act (“SCA”) allows a private right of action against anyone who “(1) willfully accesses without authorization a facility through which an electronic communication service is provided; or (2) willfully exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized unfettered access to a wire or electronic communication while it is in electronic storage in such system.” See 18 U.S.C. § 2701(a); see also 18 U.S.C. § 2707(a).

847. The Electronic Communications Privacy Act, 18 U.S.C. §§ 2510, defines an “electronic communication” as “any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce.” 18 U.S.C. § 2510(12). The SCA incorporates this definition of “electronic communication.”

848. To create the information transferred to FB such as all posts, private messages, and similar communication (collectively “FB user” information” or “content”), FB users transmit writing, images, or other data via the Internet from their computers or mobile devices to FB’s servers. This FB content, therefore, constitutes electronic communications for purposes of the SCA.

849. The SCA distinguishes between two types of electronic storage. The first is defined as any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof.” 18 U.S.C. § 2510(17)(A). The second type is defined as “any

storage of such communication by an electronic communication for purposes of backup protection of such communication.” 18 U.S.C. § 2510(17)(B).

850. FB saves and stores FB user information indefinitely in electronic storage repositories.

851. Plaintiffs did not authorize FB to share their user information with any third party.

852. Pursuant to 18 U.S.C. § 2702(a)(2), before their FB accounts were blocked by FB, Plaintiffs were users of FB’s remote computing service.

853. By definition, because FB provides the ability to send or receive wire or electronic communications, FB is an electronic communication service within the meaning of the SCA.

854. Pursuant to 18 U.S.C. § 2510(13), before their FB accounts were blocked by FB, Plaintiffs were users of FB’s electronic communication service.

855. Pursuant to 18 U.S.C. §§ 2707(a) and 2510(11), Plaintiffs were FB registered users who were harmed by FB’s violations of the SCA.

856. Because it provides computer storage and processing services by means of an electronic communications system, FB is a remote computer service within the meaning of the SCA.

857. Pursuant to 18 U.S.C. §§ 2702(a)(1) and 2510(15), FB is a provider of an electronic communication service to the public.

858. Pursuant to 18 U.S.C. § 2701(a), FB maintains facilities through which an electronic communication service is provided.

859. Pursuant to 18 U.S.C. §§ 2702(a)(2) and 2711(2) FB is a provider of a remote computing service to the public.

860. Pursuant to 18 U.S.C. § 2510(6) and 18 U.S.C. § 2707(a) FB Defendants are persons or entities within the meaning of the SCA.

861. Pursuant to 18 U.S.C. §§ 2501(12), Plaintiffs use of FB's messaging systems and transfers of information to FB constitute electronic communications.

862. Pursuant to 18 U.S.C. 2501(17), Plaintiffs' electronic communications were in electronic storage repositories.

863. Pursuant to 18 U.S.C. §§ 2701(a) and 2702(a)(1), FBs violated the SCA by allowing access to third parties to FB's information repository that stored FB user' information and electronic communications, including Plaintiff's, and by knowingly divulging the contents, including Plaintiff's', electronic communications to numerous FB authorized third parties and unauthorized third parties.

864. Pursuant to 18 U.S.C. § 2702(a)(2), FB also violated the SCA by knowingly divulging the contents of Plaintiff's' electronic communications that were carried or maintained on FB's remote computing service to numerous unauthorized third parties.

865. The contents of Plaintiff's' electronic communications that FB divulged to unauthorized parties were non-public, and Plaintiff's reasonably believed that the contents of these communications would be protected against publication to unauthorized parties.

866. The subsequent disclosure of FB user information by applications and business partners to additional unauthorized third parties was reasonably foreseeable, and FB knew or should have known about this subsequent disclosure.

867. FB also failed to effectively audit, limit, or control computer applications or business partners or numerous other third parties from accessing FB user' information so as to prevent the subsequent disclosure of that FB user information.

868. FB directly profited from the disclosure of FB user' information, through advertisements placed by unauthorized parties that received FB user information from applications or business partners, or numerous other third parties including Cambridge Analytica.

869. FB users of computer applications, such as "This Is Your Digital Life," were not aware of and did not consent to the disclosure of the contents of their electronic communications and their FB user' information and that of their "Friends" to unauthorized parties, including Cambridge Analytica, FB business partners, advertisers, and information brokers.

870. As a result of FBs' violations of the SCA, Plaintiffs have suffered injury, including but not limited to the invasion of Plaintiffs' privacy rights.

871. Pursuant to 18 U.S.C. § 2707(c), FB Defendants profited through their violations of the SCA, and Plaintiffs suffered actual damages as a result of these violations.

872. Plaintiffs are also entitled to preliminary and other equitable or declaratory relief as may be appropriate, as well as reasonable attorneys' fees, if any, and litigation costs pursuant to 18 U.S.C. § 2707(b).

873. FB's violations of the SCA were committed deceptively, willfully and recklessly and with malice.

874. Accordingly, Plaintiffs also seek punitive damages pursuant to 18 U.S.C. § 2707(c).

**COUNT SEVENTEEN-VIOLATION OF CALIFORNIA'S COMPUTER DATA ACCESS AND FRAUD ACT**

875. Plaintiffs incorporate by reference all paragraphs contained throughout this Complaint as though fully set forth herein.

876. FB knowingly accessed and without permission used Plaintiffs' content and information in order to wrongfully control or obtain property or information in violation of CPC § 502(c)(1).

877. FB' knowingly accessed and without permission took, copied, and/or used information from Plaintiffs' computers, computer systems and/or computer network in violation of CPC § 502(c)(2).

878. FB' knowingly and without permission used or caused to be used Plaintiffs' computer services in violation of CPC § 502(c)(3).

879. FB' knowingly and without permission accessed or caused to be accessed Plaintiffs' computers, computer systems, and/or computer network in violation of CPC § 502(c)(7).

880. Plaintiffs suffered and continue to suffer damage as a result of FB's violations of CPC § 502.

881. FB' conduct also caused irreparable and incalculable harm and injuries to Plaintiffs in the form of invading their privacy, and, unless enjoined, will cause further irreparable and incalculable injury, for which Plaintiffs have no adequate remedy at law.

882. FB' willfully violated CPC § 502 in disregard and derogation of the rights of Plaintiffs, and FB's actions as alleged above were carried out with oppression, fraud and malice.

883. Pursuant to CPC § 502(e), Plaintiffs are entitled to injunctive relief,

compensatory damages, punitive or exemplary damages, attorneys' fees, costs and other equitable relief.

**COUNT EIGHTEEN-VIOLATIONS OF THE CALIFORNIA  
UNFAIR COMPETITION LAW**

884. Plaintiffs incorporate by reference all paragraphs contained throughout this Complaint as though fully set forth herein.

885. The conduct of FB Defendants as alleged herein constitutes unfair, unlawful and fraudulent business acts and practices as proscribed by California's Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code § 17200.

886. FB violated Plaintiffs' privacy by allowing their FB user' information to be exploited in ways that Plaintiffs could not have been foreseen.

887. Plaintiffs interests were also violated by FB Defendants numerous deceptions.

888. Had Plaintiffs known the extent to which FB allowed their personal content to be collected, aggregated, pooled, and transferred for commercial purposes to companies such as Cambridge Analytica and numerous other third parties, Plaintiffs would not have placed their information on FB to the same extent they did, if at all.

889. FB allowed third party application developers, FB business partners, device makers and numerous other third parties to harvest Plaintiff's FB users' content and information and that of their FB "Friends" on a mammoth scale with zero notice to Plaintiffs.

890. FB had a duty to disclose the nature and extent of the harvesting of their FB user' information by third parties.



891. FB's conduct was and is unfair.

892. California has a strong public policy intended to protect Plaintiff's information privacy interests.

893. FB violated California's public policy by exploiting Plaintiffs' information without Plaintiff's informed consent.

894. FB's conduct also violated the interests protected by the Video Privacy Protection Act, 18 U.S.C. § 2710; the Stored Communications Act, 18 U.S.C. § 2701 et seq.; Cal. Civ. Code §§ 1709, 1710 and Article 1, § 1 of the California Constitution.

895. To establish liability under the unfair prong, Plaintiffs need not establish that these statutes were actually violated, although the claims pleaded herein do that.

896. FB never informed Plaintiffs of the uses of their FB user' information by FB and invaded Plaintiffs' privacy by subjecting their information to largescale third party access and plundering without Plaintiff's knowledge or meaningful consent.

897. FB's unlawful conduct included stripping Plaintiffs' privacy metainformation from their photos and videos and allowing numerous third parties to access and plunder Plaintiff's FB user information.

898. Plaintiffs could not have anticipated FB's intrusion into their privacy.

899. FB' conduct did not create a benefit that outweighs these strong public policy interests. FB's conduct benefitted FB and its business partners and numerous other third parties at the expense of the privacy of hundreds-of- millions of FB users, including Plaintiffs.

900. Additionally, the effects of FB's conduct were comparable to or substantially the same as the conduct forbidden by the California Constitution and the common law's

prohibitions against invasion of privacy, in that FB's conduct invaded fundamental privacy interests.

901. FB's conduct violated the spirit and letter of the several laws that protect privacy interests and prohibit misleading and deceptive practices.

902. The FB user' information that FB allowed third parties to access and plunder exposed Plaintiffs to an increased risk of identity theft, voter fraud, tax return fraud and allowed third parties to link their identities to other information in order to de-anonymize them.

903. FB's conduct is fraudulent. FB intentionally and deceptively misled Plaintiffs concerning the use of their FB user' information affirmatively and through material omissions regarding the privacy protection FB promised to provide.

904. FB willfully and recklessly did not disclose that Plaintiffs' FB user' information could be obtained by numerous third parties.

905. Plaintiffs have suffered significant harm due to FB' deceptive and unfair business acts and practices.

906. Plaintiffs' FB user information has tangible value.

907. FB repeatedly told Plaintiffs that they alone owned their FB user' information.

908. Additionally, because FB directly leveraged unfettered access to Plaintiffs' information in order to obtain revenues from numerous third parties, Plaintiffs have a property interest in FB's profits because FB took Plaintiff's property without compensation.

909. There is value in Plaintiffs' information that FB disseminated to FB business partners, "whitelisted" applications and numerous other third parties as demonstrated by the thirst of third parties and FB for that information.
910. Plaintiffs lost the opportunity to receive value from FB and these third parties in exchange for their FB user' information.
911. Plaintiffs' FB user' information is still in the possession of FB and numerous third parties who have used and will use it for their own advantage, including financial advantage, or have sold it or will sell it for value, making it clear that Plaintiffs' information has tangible value.
912. Plaintiffs are at increased risk of identity theft due to FB's practices concerning sharing users' information with third parties.
913. Plaintiffs may be subjected to future voter fraud, identity theft, medical fraud, and other harms.
914. The information shared with third parties allows this information to be aggregated with other information to identify and target Plaintiffs.
915. FB invaded Plaintiffs' privacy by failing to inform Plaintiffs that FB was sharing their information with numerous third parties, including but not limited to application developers, FB business partners, device manufacturers, mobile carriers, software makers, security firms, banks, credit reporting and government agencies, chip designers, retailers such as Amazon and wholesalers.

916. ' FB did not disclose the nature or the extent of the exploitation of Plaintiffs' FB content and user' information.

917. FB invaded Plaintiffs' privacy by subjecting them to psychographic marketing that exploited intimate aspects of their identity, including emotional and psychological manipulation.

918. Plaintiffs' information was exploited without Plaintiff's informed consent.

919. Accordingly, Plaintiffs are entitled to part of FB's profits that were generated by their information without informed consent.

920. Plaintiffs seek an order to enjoin FB from such unlawful, unfair, and fraudulent business acts or practices, and to restore to Plaintiffs their interest in money or property that may have been acquired by FB by means of unfair competition.

921. Section 17203 of the UCL authorizes a court to issue injunctive relief "as may be necessary to prevent the use or employment by any person of any practice which constitutes unfair competition."

922. Plaintiffs also seek the following injunctive relief: (1) an "opt in" rather than "opt out" default for sharing personal content in all of FB's user settings; (2) disclosure of the purposes of which Plaintiffs' personal content is used by FB, information brokers, device makers, mobile carriers, software makers, security firms, application developers, advertisers and other third parties with whom FB has shared users' information without their consent; (3) destruction of all personal content obtained by FB and all such third parties where such content is within FB' control or possession; (4) a complete audit and

accounting of the uses of Plaintiffs' FB user' information by third parties; (5) a permanent injunction preventing such sharing of information with these third parties without FB users' informed consent and affirmative authorization; and (6) a permanent ban on targeting Plaintiffs with advertisements or marketing materials based on information from information brokers.

## **XI. PRAYER FOR RELIEF**

**WHEREFORE**, in accord with the above paragraphs and as this Court deems appropriate, Plaintiffs respectfully request the following relief:

923. Plaintiffs request that the Court enter judgment in their favor and against FB Defendants, as follows:

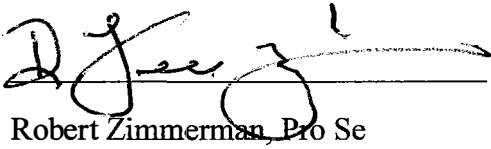
924. Enter Judgment against FB Defendants on Plaintiffs' asserted causes of action and award Plaintiffs appropriate relief, including actual and statutory damages, restitution, disgorgement, and punitive damages, equitable, injunctive, and declaratory relief as may be appropriate.

925. Award all costs, including experts' fees and attorneys' fees, if any, as well as the costs of prosecuting this action; pre-judgment and post-judgment interest as prescribed by law; and grant additional legal and equitable relief as this Court may find just and proper.

**XII. DEMAND FOR JURY TRIAL**

926. Plaintiffs hereby demand a trial by jury on all the issues so triable.

Respectfully submitted by,



Robert Zimmerman, Pro Se

Dated: August 5, 2019