Before the
Federal Trade Commission
Washington, D.C.

Complaint seeking investigation, enforcement, penalties, and other relief as appropriate against Facebook, Inc.	Submitted November 15, 2018

I. Introduction

1. On September 28, 2018, Facebook, Inc. announced that 50 million users had been compromised in a massive data breach that put their entire accounts in the hands of unknown rogue actors. An additional 40 million users also had their accounts reset due to uncertainty about the scope of the breach.

2. While Facebook, Inc. has released few details about the attack, it is clear that virtually all the information users provided to Facebook, Inc. was potentially exposed, including personal biographical data, private messages, photographs (including those uploaded but not shared), and credit card numbers. Once inside Facebook's security wall, the attackers stood in users' shoes – with complete and total control over their profiles, accounts, and social media interactions.

3. The attackers also gained access to any apps or services that the victims had linked to their Facebook account using the corporation's "Facebook Login" feature. This put Facebook-connected users of apps like Tinder, Bumble, Spotify, Uber and thousands more at risk of having their accounts hijacked and misused.

4. This breach is the latest in a long string of Facebook, Inc. privacy violations. In 2007, the company apologized for sharing private information with user friends without asking permission. In 2011, the company made false claims that users would retain meaningful control over their privacy, leading to a landmark 2011 Consent Decree with this agency. In 2013, a bug exposed emails and phone numbers. This bug

was related to uploads of user contact lists. In 2017, the massive Cambridge Analytica scandal allowed the data of 87 million user profiles to be downloaded off the platform and used to manipulate the 2016 US Presidential election and Brexit referendum.

5. The breach also comes just a few months after Facebook, Inc.'s CEO Mark Zuckerberg told the United States Congress that "we have a responsibility to not just build tools, but to make sure those tools are used for good . . . . It will take some time to work through all of the changes we need to make, but I'm committed to getting it right."

6. Facebook, Inc. has a track record of prioritizing advertising over security. In October, 2018, academics uncovered the company was using contact information handed over for security purposes, such as for two-factor identification logins or or in order to receive alerts about new log-ins to a user's account, to engage in ad targeting. The surveillance-intensive business model of targeted advertising combined with the need to secure data presents perhaps an unresolvable conflict of interest for the company as currently constituted.

7. Facebook, Inc. is a serial privacy violator that cannot be trusted. It has grown too big and its products have become too integrated and too complex to manage. Not only can we no longer trust Facebook, Inc. to manage its system safely, the corporation no longer has the capacity to do so effectively.

8. The organizations filing this Complaint seek a thorough investigation of the "View As" breach and appropriate enforcement using all available remedies against Facebook, Inc. for its apparent breaches of the FTC Act and the 2011 Consent Decree.

9. The organizations filing this Complaint also call for a broader investigation into a far more fundamental question – has Facebook, Inc. grown so large and complex that it is no longer governable at all?

II. The Freedom from Facebook Coalition

10. The Freedom from Facebook Coalition brings together diverse, non-partisan organizations representing consumers, workers, policy experts, creative artists and ordinary citizens from all walks of life demanding strong enforcement of consumer protection laws and a healthier, more open and transparent and competitive digital economy.

11. Our members include: Open Markets Institute, Citizens Against Monopoly, the Communications Workers of America, the Content Creators Coalition, Democracy for America, Demand Progress, Jewish Voters for Peace, Move On, MPower Change, Public Citizen, RootsAction, and Sum of Us.

III. Facebook, Inc.

12. Facebook, Inc., a Delaware corporation with its operational headquarters in Menlo Park, California, was founded in 2004 in Cambridge, Massachusetts by Mark Zuckerberg, Eduardo Saverin, Dustin Moskovitz, Andrew McCollum, and Chris Hughes. Facebook, Inc. owns three significant social networks: Facebook, Instagram, and WhatsApp.

13. Facebook, owned by Facebook Inc., is the largest social media network in the world with over 2 billion daily active users globally, including 214 million daily users in the United States alone. Every day its users post 55 million status updates, upload 350 million photographs, 'like' nearly 6 billion posts, and send 60 billion messages over its proprietary Messenger network. Its apps are downloaded 1.06 million times a day, and the corporation gains 400 new users every minute.

14. Much of Facebook Inc.'s growth has been fueled by mergers and acquisitions that expanded the corporation's product offerings while taking potential competitors off the field. These include the acquisition of Instagram in 2012 and the acquisitions of WhatsApp and Oculus VR in 2014. As far as we are aware, no proposed Facebook, Inc. acquisition has ever been blocked by a US regulatory authority.

15. Facebook, Inc. is currently one of the most valuable companies in the world. Fortune Magazine lists it as the 76th largest corporation in the United States by revenue, and it has a market value at the time of this filing of $406.41 billion *(as of Nov. 15, 2018)*].In the second quarter of 2018, the most recent for which data is available, it earned revenue of $13.23 billion, or $143.8 million a day.

16. The bulk of Facebook, Inc.'s revenue comes from advertising targeted at its users using data the corporation collects from multiple channels, including information users share with its social networking

subsidiaries and data it captures by tracking and surveilling user activities across the web.

17. Facebook, Inc.'s ability to mine user data and target ads is uniquely robust in the US economy, due to the corporation's extraordinary scale, the personal nature of information its users share, and the breadth of its related products and services including Instagram, WhatsApp, Messenger. Only Google has comparable scale and reach, though even Google cannot match the depth of Facebook, Inc.'s social networking data.

18. Facebook, Inc.'s data reach is further extended by its "Facebook Login" product that allows user to sign up for other apps and websites based on their Facebook credentials and without creating a new, freestanding account. Facebook captures two-thirds of the social logins for sites that use this kind of external credentialing, giving it a rich new source of data about user activities at tens of thousands of non-Facebook websites.

IV. Facebook's Repeated Breaches of its Users' Privacy and Data Security

19. The 2006 launch of Facebook's "news feed" automatically broadcast a host of user activities and updates to all their friends as a default feature without clear disclosure or consent. Mark Zuckerberg admitted at the time that "We really messed this one up" and that the corporation "didn't build in the proper privacy controls right away".

20. Facebook's Beacon advertising system, launched in 2007, tracked users' activity on third-party partner sites back to Facebook and automatically posted them to user profiles, even when users weren't logged in to Facebook and despite user efforts to opt out of the program. Facebook, Inc. ultimately paid $9.5 million to settle these claims.

21. In 2010, a Harvard Professor filed a complaint with this agency revealing that Facebook was sharing user information with advertisers including profile details and web activity without disclosure and consent.

22. In November 2011, the FTC entered into a far ranging consent decree with this agency, arising out of repeated breaches of user privacy and false claims that Facebook, Inc. would protect user information. The

charges grew out of a December 2009 change to the Facebook website that made users' private information public without their consent, and repeated Facebook, Inc. misrepresentations about the information it shared with third party apps, the it shared with advertisers, and the handling of data after user deleted or deactivated their accounts.

23. In 2011, Facebook incorporated facial recognition as a default setting on its 'tag suggestions' feature without clear disclosure or obtaining consent from users for this invasive new technology. After consumer outcry, Facebook, Inc. admitted "we should have been more clear with people during the roll-out process when this became available to them".

24. In January 2012, Facebook launched a secret experiment to manipulate user moods by feeding nearly 700,000 test subjects skewed diets of positive or negative news, without any disclosure or consent. The privacy watchdog EPIC filed a complaint with this agency about this unethical "research" study.

25. In 2013, a bug made the emails and phone numbers of 6 million Facebook users public to users who had some tangential connection to them on the site (ie. 'friends of friends'), despite that information being designated 'private' or for 'friends only'. This breach was not noticed by Facebook, Inc. but only came to light after a "white hat" hacker uncovered and reported it.

26. In what should have been a wakeup call ahead of the Cambridge Analytica, a software engineer was able to automatically scrape or harvest names, profile photos, and locations of users by entering their mobile phone numbers into the platform's "Who can find me?" feature, even if the phone numbers were set to private. By generating random phone numbers, he was able to collect data on thousands of users.

27. In 2018, it was revealed that the data of 87 million Facebook users was shared with political consulting firm Cambridge Analytica. 270,000 users took a quiz designed by Cambridge Analytica to extract users' profile information and in the process, exposed the profile information of their entire "friends' list". Cambridge Analytica proceeded to sell this data, via their consulting services, to various parties, including the 2016 Trump presidential campaign and the Brexit "leave" campaign.

28. Facebook has used phone numbers provided by users for two-factor authentication security purposes in order to target advertisements, a use they did not clearly disclose, explain, or obtain separate consent for. This follows an earlier scandal in which the corporation spammed users' two-factor authentication number with texts and then automatically posted their replies to that spam as status updates for all to see.

29. In the spring of 2018, Android users realized Facebook was using its Messenger app to track and log their texts and phone calls. Facebook, Inc. claimed users granted Facebook permission to do this when they synced their phone contacts list with the Facebook Messenger app.

30. On October 11, 2018, Facebook suspended the Russian firm SocialDataHub "because they were scraping people's data" from the site.

V. Facebook's Many Promises to Protect Users' Privacy and Keep Their Data Secure

31. Since its inception, Facebook, Inc. and Mark Zuckerberg have promised users that their data is protected, and they have complete control over their privacy on the platform.

32. In 2005, Mr. Zuckerberg said of the platform, "We're not forcing anyone to publicize any information about themselves. We give people pretty good control over their privacy. I mean you can make it so that no one can see anything, or no one can see your profile unless they're your friend."

33. A decade later, Mr. Zuckerberg responded to the NSA PRISM program's collection and use of Facebook data, writing in a personal post, "To keep the internet strong, we need to keep it secure. That's why at Facebook we spend a lot of our energy making our services and the whole internet safer and more secure. We encrypt communications, we use secure protocols for traffic, we encourage people to use multiple factors for authentication and we go out of our way to help fix issues we find in other people's services."

34. Facebook, Inc. and Mr. Zuckerberg continue to promise data security to users, even as that data is repeatedly compromised. After the Cambridge Analytica scandal, Zuckerberg wrote, "We have a

responsibility to protect your data, and if we can't then we don't deserve to serve you. I've been working to understand exactly what happened and how to make sure this doesn't happen again… We will learn from this experience to secure our platform further and make our community safer for everyone going forwar

35. In a full-page newspaper ad purchased and placed around the same time, Mr. Zuckerberg again promised to more completely protect users' data: "This was a breach of trust, and I'm sorry we didn't do more at the time. We're now taking steps to make sure this doesn't happen again. . . I promise to do better for you."

36. In April of this year, Mr. Zuckerberg testified before the Senate Judiciary Committee, emphasizing the responsibility of Facebook's developers to protect user data and once again stating the corporation was committed to stopping such breaches: "It's not enough to give people control of their information, we have to make sure developers they've given it to are protecting it too. Across the board, we have a responsibility to not just build tools, but to make sure those tools are used for good. It will take some time to work through all of the changes we need to make, but I'm committed to getting it right."

37. However, influential voices in tech including former Facebook insiders have questioned these statements and commitments

38. After selling his corporation, WhatsApp, to Facebook, Inc. 2014 and subsequently leaving the corporation a few years later, Brian Acton told *Forbes*, "I sold my users' privacy. I made a choice and a compromise. And I live with that every day."

39. Chris Hughes, a co-founder of Facebook, Inc. who left the corporation in 2007, said in response to the Cambridge Analytica scandal, "The idea that this was unforeseeable seems like a stretch. The public reckoning now is very much overdue."

40. Apple CEO Tim Cook, differentiating Apple from Facebook, Inc., warned about the platform: "[Apple has] never believed that these detailed profiles of people, that have incredibly deep personal information that is patched together from several sources, should exist. [These profiles] can be abused against our democracy. It can be abused by advertisers as well."

41. Roger McNamee, an early investor in Facebook, Inc., has spoken out at length about what the platform has become, arguing that Facebook has "behaved irresponsibly in the pursuit of massive profits" and has "consciously combined persuasive techniques developed by propagandists in the gambling industry with technology in ways that threaten public health and democracy."

42. McNamee has warned about the risk of using Facebook, Inc. to user privacy, telling CNBC, "There's been an increasing understanding that when you're using Facebook, a lot of bad things are going to happen to you, as a user. That is not a 100 percent guarantee, but the risk is really, really high."

VI. The 2018 Breach of Facebook's "View As" Feature

43. On September 28, 2018, Facebook, Inc. disclosed a major security breach that had potentially affected nearly 50 million user accounts. On October 12, the company clarified that 30 million accounts appear to have been actually compromised.

44. By exploiting a vulnerability in Facebook's "View As" feature – which allows users to see how their profiles appear to others – hackers were able to harvest highly sensitive "access tokens" that could then be used, in Facebook's words, to "take over" accounts. Facebook, Inc. describes these access tokens as "digital keys" that would let hackers pose as the user online, engage with their friends and contacts, and use or share any of their information, including private messages, pictures that had been uploaded but not shared, and payment methods.

45. In addition, because these access tokens are used to verify "Facebook Login" requests, the hackers could also access and use any linked app or third-party service, including dating sites, health portals, and message boards.

46. The potential harms of this kind of data breach go well beyond the ordinary damage caused by compromise of sensitive information. In our connected culture, being impersonated online is a deeply personal invasion that could run from the merely embarrassing – like having an unflattering photo shared – to the devastating – including lost friendships or broken relationships. The Ashley Madison breach – a

severe breach but one that did not raise the even more invasive specter of online impersonation – resulted in suicides, divorces, and job losses.

47. At this point, the toll of the Facebook "View As" breach is not known. Facebook, Inc. CEO Mark Zuckerberg stated on September 28 that "We do not yet know whether these accounts were misused." Several days later, the corporation reported it had "so far" found no evidence the access tokens were used to breach third party apps. On October 12, it revealed that extensive personal information had been breached along with access tokens, including "surname, gender, locale/language, relationship status, religion, hometown, self-reported current city, birthdate, device types used to access Facebook, education, work, the last 10 places they checked into or were tagged in, website, people or Pages they follow, and the 15 most recent searches."

48. FTC action is needed to ensure that Facebook, Inc. cannot sweep this matter under the rug with such vague and incomplete assurances. It is the only way to ensure victims of this breach have accurate information about what happened to them.

49. While European investigators have opened up their own review of this matter, it is vital for US enforcers to act as well. Facebook, Inc. is an American corporation and many US citizens were undoubtedly victims of this breach. The FTC has jurisdiction and a responsibility to protect US consumers and to set standards for the US-driven internet economy.

VII. Claims

50. The Freedom from Facebook Coalition asks the Commission to investigate and act on the following specific claims as well as any other potential violations of the FTC Act and all other authorities under its jurisdiction.

Claim 1
Breach of 2011 Consent Decree

51. In 2011, Facebook, Inc.'s violation of user privacy led them to settle with the FTC and agree to the terms of the Consent Decree finalized in 2012.

52. Under the agreement, Facebook, Inc. cannot misrepresent the privacy or security of users' personal information and is required, among other

things, to obtain affirmative consent to privacy changes, "establish and maintain a comprehensive privacy program designed to address privacy risks associated" with the operation and development of the site and related products.

53. The latest breach was the result of several errors in Facebook's "View As" feature's code, made when Facebook updated their video uploader in July 2017 – more than a year before the breach was discovered.

54. User data was exposed for 14 months, because Facebook, Inc. failed to "maintain a comprehensive privacy program" as promised in the consent decree and as promised by the corporation and Mark Zuckerberg as detailed in paragraphs 30-34 above.

55. Furthermore, Facebook, Inc. failed to inform users that system updates may compromise their data and implemented these flawed new features without the express consent of users.

56. The penalty, outlined in the consent decree, is $41,484 per user per day. This violation affected 50 million users for nearly 430 days, calling for trillions of dollars in potential fines.

Claim 2
Breach of Section 5 of the FTC Act

57. Section 5(a) of the FTC Act prohibits "unfair" or "deceptive" acts in interstate commerce.

58. Past FTC investigations including the Ashley Madison case and the LabMD case have made clear that lax data security practices can constitute unfair business practices under the FTC Act.

59. In this case, given the gravity of the risk of loss of control of accounts due to theft of access tokens, Facebook, Inc.'s failure to prevent the "View As" breach constitutes an unfair practice that violates Section 5(a).

60. Past FTC cases including the Uber case establish that misrepresentations or omissions regarding data security and privacy and failing to live up to promises made regarding the security of customer information constitute deceptive acts under the FTC Act.

61. In this case, in light of the severe "View As" breach, Facebook, Inc.'s many promises to take appropriate security measures regarding customer information, outlined in paragraphs 30-34 above, and its assurances regarding the safety and security of the "Facebook Login" feature constitute deceptive acts or practices that violate Section 5(a).

Claim 3
Call for Expanded Investigation and Report on Facebook's Privacy Abuses, Monopoly Power and "Ungovernability" under Section 6(b) of the FTC Act

62. The "View As" breach raises issues that go beyond Facebook's violation of the 2012 Consent Decree and its breaches of the FTC Act.

63. Accordingly, we call for an investigation pursuant to Section 6(b) of the FTC Act of the role of Facebook, Inc.'s market power in the internet ecosystem and the unique threats to consumers posed by its massive accumulation of data – including that supplied by users, that harvested by surveilling their activities online, and that obtained from other sources such as data brokers or corporate acquisitions.

64. This investigation should cover Facebook's use of "Facebook Login" to expand its data holdings and neuter potential competitors.

65. This investigation should review the impact of acquisitions such as WhatsApp and Instagram on the health of the social media market and the failure of meaningful alternatives to Facebook, Inc. to arise.

66. Most fundamentally, this investigation should consider the unique issues raised when corporations become as large and complex as Facebook.

67. Facebook, Inc.'s scale renders it unable to effectively manage risk within its operations. It cannot meaningfully moderate content or protect users from harassment and abuse. It is unable to keep its own promises or accurately determine whether it is adhering to commitments it has made to users, business partners, and regulators. It has become so complex and deeply intertwined with other platforms, apps, and services that no executive or engineer can responsible anticipate or evaluate the real-world consequences of policy changes or product revisions.

68. In our view, Facebook, Inc. at this scale cannot be governed in a coherent or safe fashion – one that no one could manage and that no amount of AI or clever engineering will ever successfully control.

69. The result is a corporation managed by apology. One where unfair and deceptive practices are baked into the business model – and forced upon locked-in consumers who have no alternatives in the market and no real choices but those that Facebook, Inc. gives them.

Claim 4
Request for Any Other Appropriate Enforcement
Under Any Applicable FTC Authorities

70. We ask the FTC and its professional staff to additionally conduct its own independent evaluation of the legal and marketplace implications of the "View As" breach in the context of Facebook's repeated broken promises and privacy abuses and to take any additional investigative or enforcement steps that are available to it and warranted under the circumstances to protect consumers and address the harms caused by Facebook.

VIII. Remedies

71. We urge the FTC to seek maximum civil penalties for the breach of its 2012 Final Consent Order by Facebook, Inc. as well as permanent injunctive relief, restitution, the refund of monies paid, disgorgement of ill-gotten monies, and other any other appropriate relief related to Facebook's violations of the FTC Act and any other laws or requirements within the agency's jurisdiction.

72. These remedies should include specific consideration of breaking up Facebook, Inc., and separating its advertising and social networking businesses or its discrete platforms in order to resolve the inherent conflict in running a data-based advertising businesses while being responsible for vast amounts of personal customer information and to address the poor privacy incentives created when a company holds a data-derived monopoly and has no meaningful competition.

IX. Conclusion

73. The FTC is at a landmark moment. Facebook, Inc. and the other biggest tech platform monopolies are fast breaking all traditional bounds of size

and behavior. Consumers as a result look to you for meaningful protection and enforcement – especially in the case of a serial privacy violator like Facebook that already has one outstanding consent decree under your jurisdiction. A healthy internet economy requires consumers to have basic trust and confidence in the corporations they deal with – and that in turn requires strong and steady enforcement of the basic rules of the road. In these circumstance, for the benefit of consumers, fair competition, and the internet economy itself, the Freedom From Facebook Coalition urges you to take strongest possible action.

Respectfully submitted,

_Freedom From Facebook_____

Citizens Against Monopoly

Communication Workers of America

Content Creators Coalition

Democracy For America

Demand Progress

Jewish Voice for Peace

Move On

MPower Change

Open Markets Institute

Public Citizen

Roots Action

Sum Of Us