August 17, 2018

Patient perspectives on the Facebook monopoly

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

To the Members of the Federal Trade Commission:

This is in response to the notice for the Hearings on 'Competition and Consumer Protection in the 21st Century Hearings, Project Number P181201.'' Thank you for the opportunity to submit comments on the intersection between privacy, big data, and competition.

With the help and support of cybersecurity researchers, we are offering comment on this topic from the perspective of patient communities that convene support groups on Facebook. Over the past nine years, we have formed multiple group networks on Facebook where patients convene to offer support, share stories, and exchange information about their conditions. For example, just within the hereditary cancer community, patient support groups are comprised of approximately 30,000 women and men from all over the world. Many other such groups exist for other health conditions or areas where group support is an important resource for millions of consumers. We are a small collection of patient advocates and administrators of these support groups who use the Facebook platform. In this document, we will refer to ourselves a "Group Administrators." Group Administrators on Facebook are responsible for adding new members to a group and maintaining the support group by responding to any concerns from members. Group Administrators do not have any additional rights as users of Facebook's Platform.

Facebook CEO Mark Zuckerberg's has publicly acknowledged and encouraged the use of Facebook's platform for patient groups. He has explicitly encouraged patients to connect and share on Facebook.[1] There is one core element that makes these groups a safe and supportive space: a need for **privacy**. Moderators of patient groups have typically set them to "closed," expecting that the information shared will not be made public. There is a more secure setting called "secret" that many patient communities might prefer, except that it does not allow for support groups to be found by people searching for support on Facebook.

Here are a few examples of the types of private health information that these closed support groups share with peers on Facebook:

- Questions about treatments, surgeries, and health outcomes.
- Posts that talk about painful personal experiences.

[1] Bringing the World Closer Together, Mark Zuckerberg, June 2017

- Questions about our decisions surrounding navigating surgical and health surveillance options, post-operation side-effects, and the subsequent mental and physical impact of implementing these options.
- Details that include an individual's diagnosis, staging, recurrence, and personal treatment decisions.
- Some of our participants have not yet shared their test results with their own families, partners, and friends.

This type of information that is regularly shared to our Facebook groups is sensitive and could easily be used against the individuals. For example, employment discrimination against those with cancer is so pervasive that the U. S. Equal Employment Opportunity Commission even has an FAQ page about it. Privacy is how we prevent discrimination and other misuse of that information.

Since the revelations have surfaced about breaches of privacy relating to Facebook data, our Group Administrators began to investigate how Facebook's privacy settings actually worked for these types of support groups. General details of these privacy problems are outlined below, as they pertain to the FTC's request for public comment on competition, data security, and the impact on our own groups as end-users of Facebook.

Topic 4 (a) and (b): Data as a dimension of competition. What are the effects of *competition on privacy and data security ...and the importance of this competition to consumers and users?*

Because of its overwhelming dominance in the social media arena and the lack of any meaningful competition, Facebook's platform has been the only viable online space for many patient communities all over the world to convene. As patients convening on Facebook, our data privacy problems are rooted in the the industry-wide lack of competition.

Generally, the tech industry de-incentivizes protections of our privacy, and while this impacts platforms other than just Facebook, our experience was specifically with Facebook and so that is our focus. We would like to submit evidence that Facebook does not prioritize the needs of our vulnerable support groups as a direct result of its dominance as a communications platform. Results specific to the co-signers of this letter include:

1. Patient support closed groups on Facebook lack any meaningful negotiation power when accepting privacy policies on the tech platforms where we convene, even though we have tried to discuss this with Facebook.
2. Over time, our groups have had little choice but to remain on Facebook even when their practices don't meet our privacy expectations. We will explain further details of this below.
3. We have no options to go to another platform without causing damage to our community.

4. Further, we have no commercial alternatives that might give us better negotiation power. This is because there is little space for companies to meaningfully compete with Facebook on privacy improvements.

What is the evidence of harm that we might provide in further hearings on this topic?

The harm caused to consumers by Facebook's monopoly are not theoretical. After revelations about Cambridge Analytica, patient community leaders became increasingly concerned about privacy implications for the participants in our closed support groups and we partnered with cyber security experts to assess our groups' safety.

After initial research in April 2018, some Group Administrators were shocked to discover a vulnerability in Facebook's privacy settings . This flaw affected millions of patients. Specifically, for several years, non-public user information has been downloadable by third parties without Group Administrators' express permission, and certainly unbeknownst to the group members themselves. This problem occurred because the access control features for Facebook Groups and the consent process for those access controls was and remains confusing and contrary to any basic intuitive understanding of what the word 'closed' means to a reasonable person. Before July 2018, it was possible to scrape the membership lists (identifiable names and locations) of every patient support group on Facebook, and to match this with their contact information. It was also possible for any member of a group to download the entire history of the groups' posts via Facebook's API. As a result, these groups are learning that there may have been unprecedented disclosure of their very private information, and the group members have no idea what damage or harm might result from this information leak.

In further hearings on this topic, we can explain types of harm that may occur or have occurred due to these privacy problems:

1. Potential physical harm and loss of life for closed group members, due to parties gaining the information who might be in a position to withhold treatment options.
2. Economic harm due to financial discrimination practices by insurance companies, employers, and/or credit agencies. The same concern articulated by the EEOC, but especially relevant since many members work for small companies not covered by Federal protections.[2]
3. Leaking of data to organizations and people that the original source of the data --the person--would have wanted to avoid had they understood.
4. Exploitation of Closed support group data by organizations marketing spurious treatments. This last is the one case where we have details about specific individuals harmed, and specific parties who are doing harm.

[2] Health Insurers Are Vacuuming up Details About You - And It Could Raise Your Rates. ProPublica July 2018

We can also provide documentation for some of these types of harm, including screenshots of privacy violations and abuse from malicious actors, articles, and written accounts from patient advocates who participate in support groups. The cybersecurity experts we have worked with in the past several months estimate that extensive health information associated with real names has been leaked for hundreds of thousands if not millions of Facebook users.

Articles on this topic were published in CNBC, Forbes, Fortune, The Verge, Venture Beat, and many other outlets describing various aspects of this enormous potential leakage of private information. Until and unless Facebook agrees to greater transparency or third-party audits occur, we will not know the extent to which private data were scraped, shared, and perhaps used to inflict harm to closed group members.

Support groups attempted to reach out to Facebook to address privacy concerns.

Multiple Group Administrators in our community worked with security researchers to submit a 30 page report through Facebook's White Hat Portal on May 29th, 2018, outlining the problem and demonstrating the significant harm which vulnerable Facebook users could experience as a result.

Facebook has not fully addressed the problems raised in the report. Nor have they publicly acknowledged that the design of their group features has been misleading to the patient advocates and members who expected their groups to be private. Facebook's response to the report was: "While we recently made a change to closed groups, there was not a privacy loophole."[3]

We also have extensive documentation on the specific conversation with Facebook around these issues, which we would be happy to share upon request. This includes information from Facebook itself on how they approach their privacy architecture regarding patient communities. Further, we should briefly say that our interaction with Facebook on this issue clearly indicates that it does not regard the FTC's settlement agreement or the FTC health data breach rules as being relevant in this situation. We specifically cited Facebook's obligations under those documents to no avail. We believe this should be considered under topic (5a).

Facebook has continued to publicly apologize for its mishandling of user data without fixing the underlying problems posed by its business model. Despite Facebook's public rhetoric to the contrary, support group administrators have not yet observed sufficient meaningful action to protect groups from hacking by malicious actors, and/or disclosure of non-public user information without consent.

Given the opportunity, we have reason to believe that the company will simply return to its standard practices to prioritize its revenue-generating focus over the needs of our groups' privacy: buying up competitors and further embedding itself as the social network on which nearly all social media networking must occur. We also have evidence to suggest that rather than dealing with malicious actors that might scrape and hack these groups, Facebook may simply delete our support groups or

[3] Facebook Changes Privacy Settings after Outing Members of a Closed Medical Support Group, The Verge, July 2018

allow them to be deleted by malicious actors .[4] In contrast, given Facebook's size (2 billion users) and worldwide dominance, one has to ask how severely its revenue would be impacted if instead of allowing the scraping that may have occurred here, a more private model were developed for certain types of groups for whom privacy is critical.

[4] How a Facebook Group for Sexual Assault Survivors Became a Tool for Harassment, Wired, July 2018

Patient support groups do not have good alternatives to Facebook.

Patient support groups do not have any real option to move to another platform, as described in more detail below.[5] And yet, consumers who participate in these private groups continue to be vulnerable to harm due to the deceptive design of group settings and the unfavorable terms of service that we must accept in order to convene on Facebook's platform.

As a result of a growing awareness of significant privacy violations, closed group moderators and users find themselves in the position of having to choose between leaving Facebook and giving up the cherished communities which provide critical, daily, help to individuals, and that the Group Administrators have worked for years to build. Leaving these groups is not a viable option considering the life-saving support that many people access through these groups. Therefore we remain on Facebook, knowing our personal health (and other) data are not safe and are, in fact, perhaps being shared without consent or stolen at any given moment.

There are four reasons why patient communities cannot simply "leave" Facebook.

First, there is no way to export data as a group and migrate to a different platform. Facebook provides individual users the tools to leave with their individual data, but they ensure that communities as a whole cannot leave easily. To migrate a group to another platform, even if one became available, would mean rebuilding the group knowledge and collected wisdom from scratch, even if it could be arranged to migrate thousands of people simultaneously to a new platform. These patient communities would essentially lose 10 years of their history, compromising their ability to refer to old solutions for new members.

Second, even the departure of current groups does not solve the privacy problem for all consumers. If support groups leave the platform, then new support groups would form on Facebook in their place and unknowingly be victimized by the same harm that their predecessor groups have experienced.

Third, patient support groups face the same unfavorable negotiating terms with any new platform we might choose. We remain especially concerned about Amazon, Facebook, and Google as it becomes increasingly clear that any service they offer quickly becomes the only one of its kind, leaving consumers at the mercy of entities that prioritize growth at any costs, with monopolistic ambitions, over consumer safety and well-being.

[5] I Can't Jump Ship from Facebook Yet, New York Times, April 14th 2018

What do consumers prefer?

Addressing topic (4c): whether consumers prefer free/ad supported products to products offering similar services or capabilities but that are neither free nor ad-supported;

From the perspective of these support groups, preference for free vs non-free and ad-supported vs not ad-supported is not relevant and is premature. The ad-supported Google and Facebook search capabilities ensure that support seekers never even see competitive options that do not involve these platforms. The reason that ad-supported models are problematic is that they allow platforms to control the underlying flow of people on the internet, usually by deploying layers of so-called "dark UX patterns" to ensure that the ad-driven model self-sustains. Fees paid by users to access these platforms would not matter if the users did not have as a result much better control over the automated rules of the platform.

It does not matter if a single person insists on privacy by refusing to use Facebook, for then they simply give up the ability to communicate with other people who share their medical condition because those other patients all "gave in" and use Facebook.

This means that there is a large community of patients who only use Facebook to access the support offered by our patient support group, and others like us. We are concerned that there are users who use Facebook, despite mistrusting the company, only because our support community cannot be accessed without it. If the FTC would like more information on this, we can provide specific data to this effect. We believe this discussion applies to both question (4) and (3) of your notice.

Facebook's Privacy Commitments:

There are two important factors to consider when looking at Facebook's commitment to privacy, terms of service, and communication on these topics to users:

- What were the privacy commitments made to people joining the groups and were they clear?
- Was the level of security provided reasonably designed to enable the company to fulfill its commitments to group users?

Important details pertaining to closed group API were never clearly communicated to Group Administrators or to Facebook's users in their Terms of Service. Facebook's terms have changed significantly over time since the founding of these groups.

For example, one of the longest standing support groups for hereditary cancer - BRCA Sisterhood - started in 2009. Facebook launched their API in 2010, after the group became entrenched on the platform. At no time since the API was launched have these non-technical Group Administrators and

group members ever been given a clear communication about how the Group API and screen scraping tools could be used to gather vast amounts of non-public user information.

We'll cite a very specific example here with reference to the group API documentation. Since 2010, the sparse developer documentation did not adequately explain the privacy implications to a non-technical audience.[6] Specifically if one looks at older versions of group API documentation, there is one simple line to explain massive implications for group admins and their members. Under the heading"For Public and Closed Groups" the permission simply states: "A User access token of an Admin of the Group."

These older versions of the documentation have now been deprecated after the API shut down on April 4th. It took a great deal of research and testing the API for group administrators to fully understand what this simple line actually meant for them: i.e., *that any user in their group could grant an access token to any developer in order to read all the posts, photos, comments and history of all their support members.*[7] Some of these group features evolved over time, and we question whether this sparse documentation may have been misleading by design.

What are the benefits and costs of regulations?
[we raise this point with reference to (4)*(d) and (e)]*

Consistent regulation may be helpful in addressing some of these concerns. Specifically, compatibility with GDPR should be considered, especially given that the tech industry is already moving to comply with these regulations in Europe. Both GDPR and HIPAA provide a right for consumers to understand how their personally identifiable data is being shared. While we do not advocate that social media platforms be regulated under HIPAA, having a "HIPAA compatible" way to acquire "disclosures" as well as rights to copies of data maintained by companies regarding a given user are elements of both GDPR and HIPAA that should be part of any attempt to further regulate large social media platforms. Currently, US citizens have no leverage to force Facebook or other similar companies to detail how their data were shared with third parties. We asked for such an accounting, and so far we have been ignored.

Furthermore, there are a range of countries in which consumer privacy protections and policies are working well, while encouraging innovation through competition. We propose that the FTC examine these models to inform policy in the US. Technology innovation can and does flourish in more carefully regulated information markets. Israel, for example, imposes greater privacy and cybersecurity requirements on its technical community than does the U.S. and yet they continually release innovative technology solutions. Again, we do not recommend that social media companies be regulated under HIPAA, but HIPAA does represent a stringent US-based privacy regulation that has not blocked companies from providing technical innovation. Companies frequently claim otherwise, stating that HIPAA is a barrier to innovation, but in reality HIPAA can and is being navigated successfully by the high tech community.

---

[6] See full history of Group API developer documentation here.
[7] The impact of user access tokens on groups was only discovered after reading Facebook's developer blog post on April 4, 2018 about changes to the platform. Specifically the line: "Going forward, all apps will require explicit admin authorization."

GDPR gives rights to consumers to understand how a company is sharing their data with other organizations. So far, Facebook has not been willing to provide an accounting of which non-group-member Facebook users have downloaded data from a given patient support group. However, European members of our community will make requests under GDPR so that the entire community will be able to infer how our patient data is being shared. It is reasonable to expect US citizens to have the same right to transparency in the interests of fair practices for consumers as citizens in the EU. Transparency cannot be unduly burdensome where platforms like Facebook must already be transparent for their European users.

As Facebook's services become more personal and ubiquitous, the failures of poorly designed privacy policies will continue to have an outsized impact on vulnerable populations, unless the FTC intervenes.

We would be happy to provide more detailed information about the topics discussed in this letter and look forward to the opportunity to do so. Thanks for this opportunity to share our concerns and experience through this FTC notice.

Sincerely,

Fred Trotter, Cybersecurity Researcher
Shoshana Schwartz, BRCA Sisterhood (FB Group Administrator)
Lisa Guzzardi, RN & Curator/Administrator of BRCA Advanced 101 & 102 Journal Club on Facebook
Lisa Cohen, Founder of Bracha Israel (FB Group Administrator)
Matt Might, Cybersecurity Researcher, NGLY1 Community Advocate, Director of the Hugh Kaul Precision Medicine Institute
Karl Surkan, Participant Representative to All of Us Research Program, Founder of Transrecord (FB Group Administrator)

Note: Because this response covers questions across 3, 4 and 5, we are submitting duplicate copies to each submission URL.