December 14, 2018

ATTN: REDACTED (Name)
Division of Privacy and Identity Protection
Federal Trade Commission

Dear REDACTED (Name),

Over an extended period of time, Facebook deceptively solicited patients to use its “Groups” product to share personal health information about their health issues. Facebook has marketed this product as a Personal Health Record. Facebook then leaked to the public health data that those patients uploaded. At least in some cases, this was done contrary to the specific privacy decisions made by Facebook users.

Sharing of privately posted personal health information violates the law, but this serious problem with Facebook’s privacy implementation also presents an ongoing risk of death or serious injury to Facebook users. Facebook has ignored our requests to fix the specific issues we have identified to the company, and denies publicly that any problem exists. All of this represents unfair, deceptive and misleading interactions between Facebook and its users in violation of the FTC Act. Specifically, Facebook:

A. Actively solicits and uses AI to nudge individuals into joining Facebook patient support Groups, even though users do not understand the manner in which Facebook uses the user’s own private information to make those suggestions.
B. Explains its privacy policies to group users in an unfair, deceptive and misleading way, violating the FTC Act.
C. Offers a personal health record (PHR) from which identifiable health data leaked out, which it then failed to disclose, violating the FTC breach reporting rule, and putting patients at risk.

All of these actions also violate Facebook’s 2012 consent order, as the FTC is likely already investigating.

The report first offers an in-depth review of the health data being shared, used and curated in these Facebook Groups; second, illustrates Facebook’s unfair practices, and third, explains why the Facebook Groups platform should be regulated as a PHR.

Along with this submission, we are providing copies of our communications with Facebook on these topics, as well as their formal responses to us in reply. Those documents provide more detail on the mechanism of action for the data leaks that we reported to Facebook.

Thank you,
Fred Trotter & David Harlow
Co-Signed By: Patient A & Patient B, BRCA Community Advocates; Matthew Might, NGLY1 Community Advocate

FTC Complaint:

Multiple Ongoing Patient Privacy Breaches in the Facebook PHR (Groups Product)

Table of Contents

Brief Timeline

This timeline briefly discusses our failed efforts to get Facebook to change its privacy architecture to protect patients from the disclosure of their healthcare information on their PHR (Groups) platform.

- March 2018: patient advocate Patient A researches patient privacy on Facebook after the Cambridge Analytica breach causes her concern about the safety of her patient community, which convenes on Facebook using the Groups product. She discovers several problems, including the ability to download the membership list of Closed or Public Facebook Groups using a chrome extension called grouply.io. She reaches out to security researcher Fred Trotter to discuss her concerns.
- April 21st, 2018: Using grouply.io, Trotter downloads the real names for the entire membership list (over 10,000 names) of the REDACTED Facebook Group. All members of this Group are positive for the BRCA mutation. Most of the names on the downloaded list include email addresses, city of residences and employers of the women who participate in the Facebook Closed Group.
- April 22nd, 2018: Trotter confirms the vulnerability, which we refer to in this report as Strict Inclusion Closed Reverse Lookup Attack (SicGRL). As a cybersecurity expert, Trotter confirms that it represents a life-threatening vulnerability in the Facebook privacy architecture.
- May 29th, 2018: Following Facebook's responsible disclosure policy, Fred Trotter, Patient A and multiple other patient community members submit the full report of the SicGRL vulnerability to Facebook. This report explicitly states that Facebook's Group product counts as a PHR under FTC rules, and explicitly reminds Facebook that the breach notification rules and deadlines apply.
- June 12th, 2018: The 10-business-day deadline for reporting the PHR breach to the FTC passes.
- June 20th, 2018: Facebook responds to the SicGRL submission. The Facebook Response indicates the security team will not commit to fixing the problem and did not acknowledge the issue as a privacy or security vulnerability.
- June 26th, 2018: In response, the team replied and enclosed an Open Letter to Facebook from BRCA Community Administrators, reiterating the seriousness of the vulnerability.
- June 28th, 2018: The 60-day deadline for notifications of users impacted by the breach passes. No member of the REDACTED Facebook Group received a notice that Fred Trotter downloaded their real names and the fact that they are BRCA positive.
- June 29th, 2018: BRCA Community advocate, Patient B, discovers that Facebook Groups Membership is no longer "world readable". This change means that although SicGRL is still a problem, it is no longer trivial to exploit at scale. Because the vulnerability can no longer easily lead to a mass-casualty event, Trotter and Patient A start discussing the problem publicly with reporters.
- July 12th, 2018: Facebook publicly denies that a Facebook privacy breach has occurred, in statements to a CNET reporter.

Facts

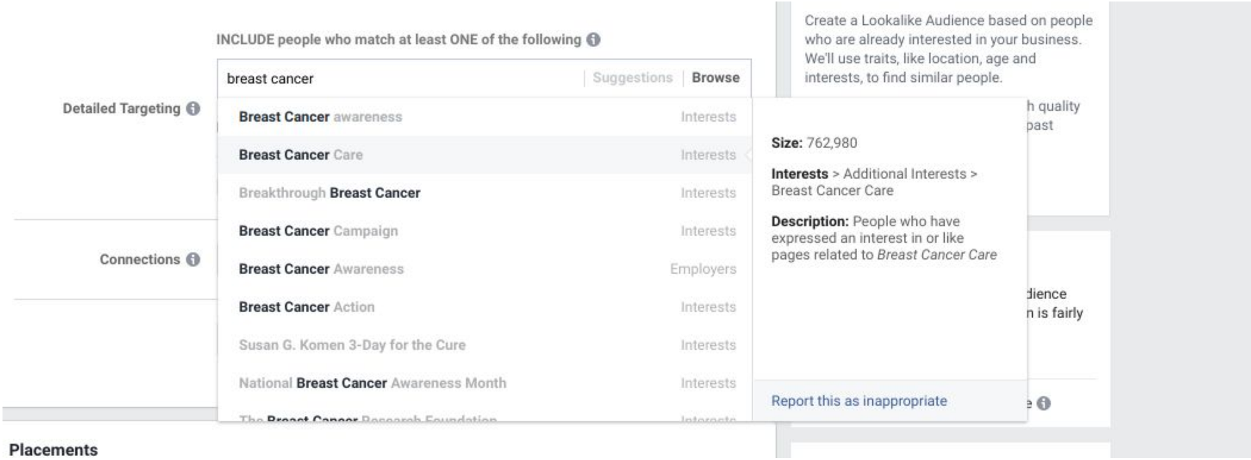
Facebook actively solicits patients to use its Groups products to share health information.

1. Facebook promoted the specific Group “REDACTED Support Group” at its first communities summit, specifically labeling the Group as a “safe place”.
   Facebook produced a video about the “Affected by Addiction Support Group” that specifically showed their Group as being connected with an Alcoholics Anonymous meeting. By correlating the Facebook’s Group with AA’s famous anonymity, Facebook communicated to prospective group members that their identities would be equally anonymous to the public.
2. Facebook has a “Support” Group type. Facebook “Group types” include “Parents”, “Project”, “Club”, etc. The “support” type, along with a clinical topic is an indication that Facebook intends for the Groups product to be used as part of healthcare treatment .
3. Mark Zuckerberg has demonstrated in multiple public forums that he is aware of and encourages the use of the Groups product for patient care collaborations and coordination.
4. In February of 2018 Jennifer Dulski, the head of “Groups and Community” at Facebook, specifically endorsed a Support Group on Facebook for addiction in an ABC News interview.
5. In August of 2018 (notably, after we indicated to Facebook that it should consider their Groups a PHR product) Facebook promoted a Group for the parents of transgender children as it promoted its new “mentorship” feature. Gender and sexuality, especially when it affects healthcare choices, is personal health information, which means that Facebook continues to promote its “support” Group product as protective of personal health information. This is especially true for transgender minors, even those with the support of their parents. Trans children and teens have high rates of being bullied and harrassed, and high rates of suicide, making privacy a paramount safety issue for this user community.
6. Facebook’s leadership and Mark Zuckerberg were directly aware of these facts in the context of health Groups (later we list public statements made by Zuckerberg that demonstrate this). Specifically, we have evidence that Zuckerberg had in-person discussions about the privacy-related issues with health information shared within Facebook Groups at a summit in 2017.

While Facebook continues to explicitly advertise that its Group products are a good way for patients to communicate their health information, this is not the primary way that Facebook works to ensure that Facebook patient communities attract new members. Facebook uses its artificial intelligence and machine learning technology to ensure that users with healthcare conditions are connected with specific Groups that support those healthcare issues. Further, Facebook allowed targeting of users' identifiable health information for Facebook's own commercial purposes--specifically allowing advertisers to connect with users with an interest in specific clinical conditions. In some cases, this enabled advertising specifically to patients and caregivers.

Below we provide screenshots and examples.

SCREENSHOT 1: Example of Ad targeting tool with a specific disease for commercial purposes.



Detailed Targeting

INCLUDE people who match at least ONE of the following

breast cancer

Breast Cancer awareness	Interests
Breast Cancer Care	Interests
Breakthrough Breast Cancer	Interests
Breast Cancer Campaign	Interests
Breast Cancer Awareness	Employers
Breast Cancer Action	Interests
Susan G. Komen 3-Day for the Cure	Interests
National Breast Cancer Awareness Month	Interests
The Breast Cancer Research Foundation	Interests

Size: 762,980

Interests > Additional Interests > Breast Cancer Care

Description: People who have expressed an interest in or like pages related to *Breast Cancer Care*

Connections

Placements

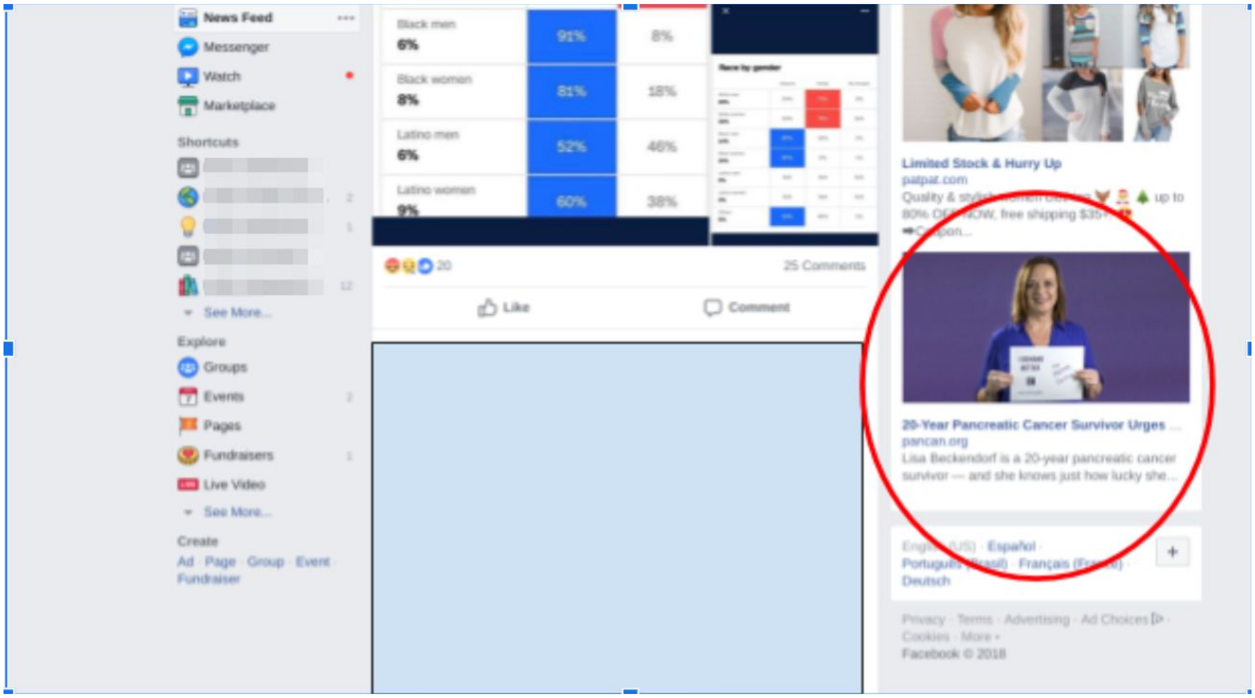
Create a Lookalike Audience based on people who are already interested in your business. We'll use traits, like location, age and interests, to find similar people.

h quality
past

dience
n is fairly

e

SCREENSHOT 2: Example of targeted ad for a health condition.



News Feed
Messenger
Watch
Marketplace
Shortcuts
See More...
Explore
Groups
Events
Pages
Fundraisers
Live Video
See More...
Create
Ad · Page · Group · Event · Fundraiser
Race by gender
20
25 Comments
Like
Comment

Black men 6%	91%	8%
Black women 8%	81%	18%
Latino men 6%	52%	46%
Latino women 9%	60%	38%

Limited Stock & Hurry Up
patpat.com
Quality & stylish women clothing 🦌🎅🌲 up to 80% OFF NOW, free shipping $35+🎁 ➡Coupon...

20-Year Pancreatic Cancer Survivor Urges ...
pancan.org
Lisa Beckendorf is a 20-year pancreatic cancer survivor — and she knows just how lucky she...

English (US) · Español · Português (Brasil) · Français (France) · Deutsch
+
Privacy · Terms · Advertising · Ad Choices · Cookies · More
Facebook © 2018

These ads provide a specific mechanism by which the Facebook platform can profit from the clinical details it data mines from its user base. Facebook makes money by offering its users a personal health record (PHR) product, and then selling information it learns about its users with the PHR context.

The impact of Active Solicitation and AI Guiding on Vulnerable Consumers

All of Facebook's solicitation, guiding and "nudging" mean that if a user has ever searched Facebook for a health topic, then the Facebook AI algorithms will continually suggest for that user to join healthcare Groups that target that clinical topic. For example, after a search for "depression" it will continually suggest that a user join depression support Groups.

Because few Facebook users understand in detail how Facebook's algorithms work, users are unaware of the extent to which the health information they expose is then used by Facebook. Because this problem represents a complex user interaction, we have made a video that details the problems.

Video: VIDEO LINK RELEASE DELAYED How Facebook leverages users actions on its platform to push patient-users into its healthcare Groups products.

How are Group Suggestions made?

We know for certain that Facebook's "Group suggestion" feature is powered by previous searches that a user has made on the platform. This is what we demonstrate in the video above. We further believe that all of the following information is used as ingredients in the "Group suggestion algorithm."

1. A user's own searches on Facebook
2. Visits to Facebook Pages that relate to a given healthcare topic (i.e., going to the page for American Cancer Society at https://www.facebook.com/AmericanCancerSociety/)
3. Visits to outside websites focused on a given healthcare topic, such as American Diabetes Association at http://www.diabetes.org/, that has Facebook's web tracker included
4. "Like" events on other people's contents (e.g., a user "likes" content on the Facebook page of a friend or family member who is undergoing treatment)
5. The content of a user's own posts on Facebook

Our investigation convinced us that these data sources are fed through an AI suggestion engine. This engine, in turn, is capable of natural language processing and topic-linking, so that suggestions can be made to the individual that connect information that is not clearly health-related to information that is clearly health-related. For instance, if a user visits a site that covers "keto", a high-protein diet that is popular among people with diabetes. It has a Facebook tracker, so Facebook then suggests that the user join a diabetes diet Group. It is possible that this is happening without human intervention, so that there is no one at Facebook who is explicitly aware that this is occurring on a topic-by-topic basis. It’s just that people who visit site A, are more likely to join Facebook Group ‘Z’, so ‘Z’ is automatically promoted to anyone who visited website A. As for explaining this to Facebook users, this specific paragraph is indeed complex, but steps 1-5 above are not. Given that Facebook has an active business model of soliciting and “nudging” people to join Groups about their health, Facebook ALSO should clearly, fairly, and in a non-misleading manner, explain how components 1-5 are used to guide Facebook users who might otherwise not join healthcare Groups.

Facebook spends a very large amount of money on “nudges” into Clinical Groups

In this complaint, we frequently refer to the UX details as “nudges” for want of a better way to describe the constant bombardment of UX elements to direct users to join specific Groups. To quantify this, it is important to note that screen real-estate, for suggesting anything to Facebook users is a zero-sum game. Any screen space that is used to promote specific Groups cannot be used for anything else.

In this zero-sum environment, Facebook promotes Groups approximately the same amount as it does “for-pay” advertisements in its web-based interface. Facebook makes most of its money, almost $4 billion a year, from these advertisements.

This means that Facebook believes that convincing its users to participate in “relevant” Groups is roughly equivalent in value to the $4 billion it makes on ads.

Using this metric, if we knew what percentage of the time, for the average user, Facebook promotes clinical Groups (as opposed to some other Group), we could calculate a metric of how much money Facebook has spent promoting its PHR product.

So the “Nudge Spend Metric” is specifically:

Ratio of the promotions of Groups to showing Ads x
Total amount Facebook earned showing Ads x
Average percent of time the Groups promoted were for clinical support Groups specifically x
=
Approximate number of dollars lost by Facebook “nudging” users into its PHR product.

We expect this number to easily be higher than $10 million, and probably higher than $100 million, per year.

Facebook describes its privacy controls for Groups in a misleading way.

There are four mechanisms by which Facebook makes privacy assertions to Group members and Group Administrators which are false and/or offer conflicting information:

- Privacy information in the Group descriptions
- Privacy information in the questions asked by Group Admins during signup
- Privacy information in the rules that Group Admins expose during signup
- Privacy information in the announcements of a Group or in pinned Group posts

The last two are especially important, because they frequently provide contradictory information to what Facebook says on the same screen. Sometimes, the Group Admins are communicating information about rules that are not enforceable, and sometimes Facebook is itself communicating incorrect information.

Below we supply three of the most common types of these misrepresentations about Facebook's Privacy rules. Also, we are providing a link to a video we made that explains this problem.

Video: VIDEO LINK RELEASE DELAYED Demonstrating the conflicting privacy messages users receive from Group Administrators and Facebook.

Facebook misrepresentations about the Group product

Example 1: "Affected by Addiction" Facebook Support Group

The Affected by Addiction Community Facebook Group description says "*This is a private group, so nothing you post will be seen by anyone outside of this group*." There is no such thing as a "private group" as Facebook makes clear elsewhere. There is a reason that no group type comes with this label.

Facebook in its data policy says "You should consider who you choose to share with, because people who can see your activity on our Products can choose to share it with others on and off our Products, including people and businesses outside the audience you shared with." This specific Group was promoted by Facebook during the communities summit and again endorsed in the ABC News interview.

Specifically from the "Our First Communities Summit and New Tools For Group Admins":

> *Matthew Mendoza, who started Affected by Addiction Support Group. The group is a safe space for people who are experiencing or recovering from drug and alcohol addiction, as well as their friends and family, to offer support and share stories.*

Underlines are ours.

In the article that promoted this the Affected by Addiction Group on ABCnews.com Facebook spokesperson Jennifer Dulski said the following.

> *Jennifer Dulski, the head of community and groups at Facebook, added that many may feel more comfortable openly discussing addiction online because of how it still carries a stigma.*
>
> *"Addiction is really somewhat a taboo topic that people don't talk about much," Dulski said. "So being able to find that community online allows people to open up."*

Example 2: "Mama Dragons" Facebook Support Group

As briefly mentioned above: In August of 2018 (notably, after we indicated to Facebook that it should consider their Groups a PHR product), Facebook promoted a Group for the parents of transgender children as it promoted its new "mentorship" feature.

The Mama Dragons Facebook Group description makes the same assertion "*As with most closed Groups, conversations including names may NOT be shared outside the group.*" This is the same contradiction with Facebook policy made by the Group above. Specifically, Facebook says in its privacy policy that the content posted to the Group products can be reshared. This group is saying the opposite.

The Mama Dragons Facebook Group description also says "*Real names must be used. It is expected that all profiles are real and individuals are accurately representing themselves. Pseudonyms are only permissible in extreme circumstances as approved by administrators.*" But the Facebook Real Name policy says that real names must always be used on Facebook, specifically "*Facebook is a community where everyone uses the name they go by in everyday life.*"

The Mama Dragons Group was promoted as part of the launch of the Facebook Groups mentorship product.

Example 3: Facebook Misrepresents "User Control" within Closed and Secret Groups.

Another, separate source of deception is Facebook's use of the phrase "users can control what other users see." Facebook implies with this statement that "users can control what other users see *while using the Facebook platform.*"

What they really mean is "You can control which users have the opportunity to copy, download and disseminate" the data that you upload to Facebook. Essentially, Facebook encourages you to think about sharing as a "one-step-through-Facebook" decision - rather than thinking about "sharing" as "many-step-many-platform" decision. Essentially, Facebook encourages users to ignore "resharing" off platform, even though this is explicitly allowed by Facebook data policies.

This perception of "user control" is problematic when there are **"Suck Puppets"**[1] who have easy access to information shared within a Closed or Secret Group on Facebook's platform. Specifically, when a user within a Closed Group shares private information in a Closed or Secret group, these data can be easily copied or downloaded to enumerable other users, platforms and mediums. Other users include Suck Puppets who can download data from a Closed Group against an individual member, depending on the screening practices of the Group administrator. Facebook's terms of service reflects this more substantial underlying reality, but everything else they communicate through their user documentation, features, and public statements encourages users to make privacy decisions as though the data cannot be copied easily off the platform.

Despite users' expectations, it is very easy to copy data off the platform. Facebook has a policy that restricts the use of "automated" tools to download content from Facebook (a rule that is obviously ignored by any bad actor, including all Suck Puppets). But as long as data was not obtained using "automated means" there is no restriction on how data can be used or shared once it is downloaded by any user.

For instance, Facebook's rules allow anyone to re-publish screenshots that are downloaded from Closed and Secret Facebook Groups. Of course, it is impossible to provide technical mechanisms to prevent screenshotting of any software. However, different sites have very different policies in place about what content downloaded from the site can be republished. Facebook's current policy explicitly allows screenshots, and anything else that is downloaded, to be liberally republished. This of course gives rise to sites that exist only to republish data that has been copied from Facebook's interface, including the sub-reddits:

- Insanepeoplefacebook
- Facebookwins
- FacebookCringe

[1] For the purpose of this document, we define the term "Suck Puppet" as a "a Facebook user account that exists only to download data about other legitimate Facebook users".

To be clear, screenshotting may be technically impossible to prevent, and republishing screenshots may be practically impossible for any site to stop. Yet, Facebook's current policy explicitly permits the taking and re-publishing of screenshots. While we remain far more concerned at the cybersecurity implications of clinical data downloaded about Facebook users at scale, the policy contrast on screenshots serves to illustrate the contradictory underlying position that Facebook has taken regarding "resharing".

Group Administrators are unknowing collaborators in sending mixed privacy messages

We should be clear that for the most part, Facebook Group Administrators seem to be well-meaning as they contradict Facebook's policies and privacy settings. We have not seen many cases where it is obvious that a Group administrator is intentionally confusing other Facebook users. Rather, the Administrators' expressions regarding Group privacy is based on their own lack of understanding about how privacy settings in Closed Groups really work on Facebook.

However, it is also true that many, if not a majority, of the healthcare related Groups on Facebook have privacy policy information that profoundly contradicts the privacy controls that Facebook actually provides for Groups.

The group descriptions on Facebook are authored by users who should be very familiar with Facebook's privacy policies, yet they typically contradict Facebook's privacy policies. These writing samples represent a pristine sample of the confusion with Facebook's privacy settings are understood by Facebook users. Not only does Facebook put no effort into correcting this misinformation regarding its privacy settings, it uses participation in Groups to drive its user data mining efforts.

Facebook knowingly allows Group Administrator users to confuse other users regarding the privacy and safety of its platform so that Facebook can profit from hyper-targeted ads.

Facebook's Groups product is used as a Personal Health Record.

The Facebook Groups product fits the legal definition of a personal health record (PHR), and Facebook fits the definition of a "vendor of personal health records" subject to the FTC's health breach notification rule, 16 CFR Part 318. (A personal health record is defined as "an electronic record of PHR identifiable health information on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual;" a vendor of PHRs "offers or maintains" PHRs, as Facebook does.) When PHI leaked from Facebook, the company had an obligation to comply with the FTC's Breach Notification Rule. Facebook did not notify affected users within the required 60 days and we believe that Facebook has not notified the FTC of the breach within the required 10 business days.

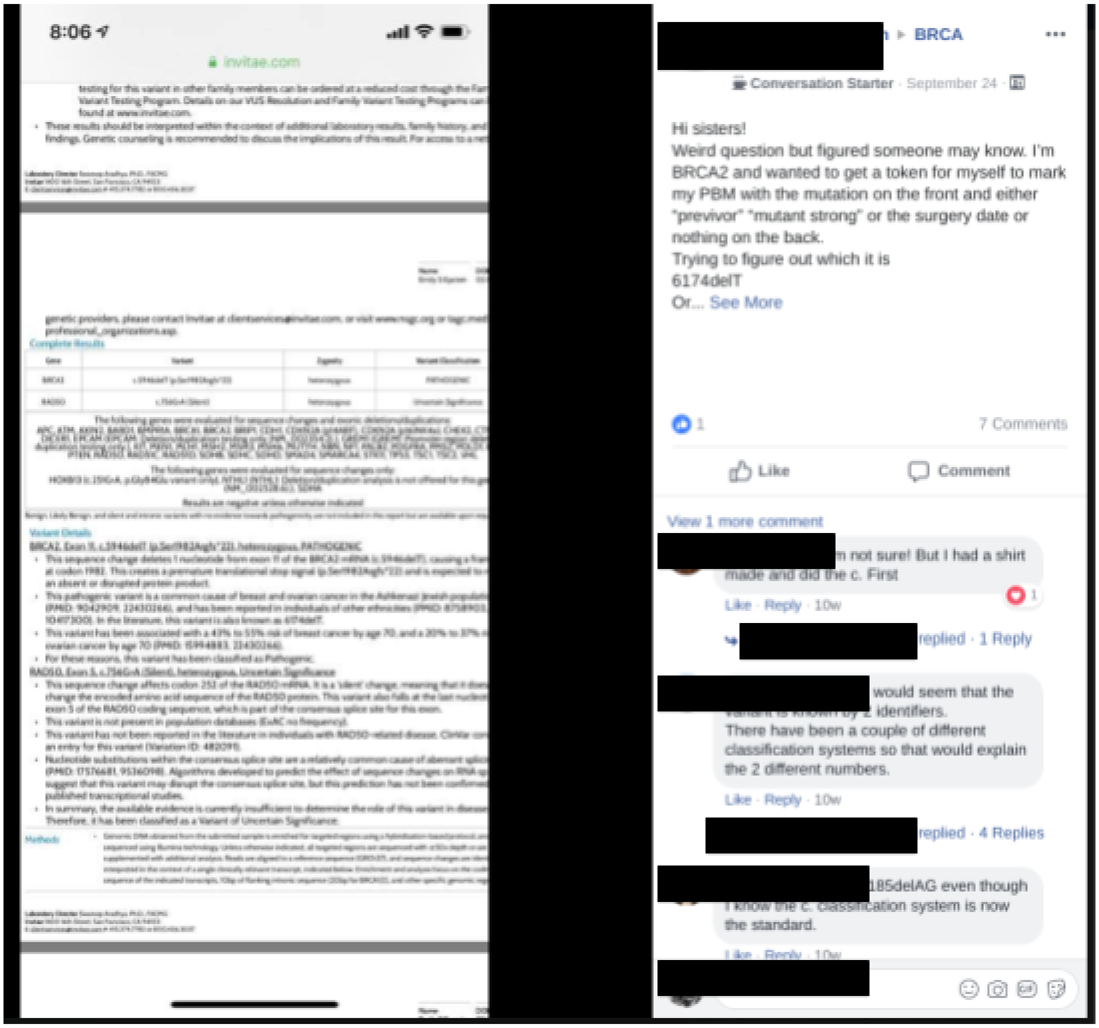
Facebook makes it simple to share information in Groups using multiple mechanisms, including check-in to a particular location (e.g., a hospital), uploading a file (e.g., a pain journal or lab result) or creating an event (e.g., a celebration of the end of chemo). However, the most common mechanism for sharing data among patients, and between patients and healthcare providers on Facebook, are videos, photos, posts, and comments, which users post to their clinical support Groups.

The sections below provide screenshots and examples of health information being collected, used, and shared.

Screenshot 1: Example of Post-Surgical Mastectomy Photo Shared in Closed Group

REDACTED

Screenshot 2: Clinical Report shared in a Closed Group



testing for this variant in other family members can be ordered at a reduced cost through the Fam
Variant Testing Program. Details on our VUS Resolution and Family Variant Testing Programs can
found at www.invitae.com.

- These results should be interpreted within the context of additional laboratory results, family history, and
findings. Genetic counseling is recommended to discuss the implications of this result. For access to a net

Laboratory Director: [illegible]
Invitae [illegible] San Francisco, CA [illegible]
E: clientservices@invitae.com [illegible]

Name
[illegible]

genetic providers, please contact Invitae at clientservices@invitae.com, or visit www.nsgc.org or logc.med
professional_organizations.asp

Complete Results

Gene	Variant	Zygosity	Variant Classification
BRCA2	c.5946delT (p.Ser1982Argfs*22)	heterozygous	PATHOGENIC
RAD50	c.756G>A (Silent)	heterozygous	Uncertain Significance

The following genes were evaluated for sequence changes and exonic deletions/duplications:
APC, ATM, AXIN2, BARD1, BMPR1A, BRCA1, BRCA2, BRIP1, CDH1, CDKN2A (p14ARF), CDKN2A (p16INK4a), CHEK2, CT
DICER1, EPCAM (EPCAM: Deletion/duplication testing only), [illegible] GREM1 [illegible]
duplication testing only), KIT, MEN1, MLH1, MSH2, MSH3, MSH6, MUTYH, NBN, NF1, PALB2, PDGFRA, PMS2, POLD1, [illegible]
PTEN, RAD51C, RAD51D, RAD50, SDHB, SDHC, SDHD, SMAD4, SMARCA4, STK11, TP53, TSC1, TSC2, VHL

The following genes were evaluated for sequence changes only:
HOXB13 (c.251G>A, p.Gly84Glu variant only), NTHL1 (NTHL1 Deletion/duplication analysis is not offered for this ge
(NM_001128611), SDHA

Results are negative unless otherwise indicated

Benign, Likely Benign, and silent and intronic variants with no evidence towards pathogenicity are not included in this report but are available upon req

Variant Details

BRCA2, Exon 11, c.5946delT (p.Ser1982Argfs*22), heterozygous, PATHOGENIC

- This sequence change deletes 1 nucleotide from exon 11 of the BRCA2 mRNA (c.5946delT), causing a fra
at codon 1982. This creates a premature translational stop signal (p.Ser1982Argfs*22) and is expected to r
an absent or disrupted protein product.
- This pathogenic variant is a common cause of breast and ovarian cancer in the Ashkenazi Jewish populatio
(PMID: 9042909, 12430266), and has been reported in individuals of other ethnicities (PMID: 8758903,
10417300). In the literature, this variant is also known as 6174delT.
- This variant has been associated with a 43% to 55% risk of breast cancer by age 70, and a 20% to 37% r
ovarian cancer by age 70 (PMID: 15994883, 21430266).
- For these reasons, this variant has been classified as Pathogenic.

RAD50, Exon 5, c.756G>A (Silent), heterozygous, Uncertain Significance

- This sequence change affects codon 252 of the RAD50 mRNA. It is a 'silent' change, meaning that it does
change the encoded amino acid sequence of the RAD50 protein. This variant also falls at the last nucleot
exon 5 of the RAD50 coding sequence, which is part of the consensus splice site for this exon.
- This variant is not present in population databases (ExAC no frequency).
- This variant has not been reported in the literature in individuals with RAD50-related disease. ClinVar con
an entry for this variant (Variation ID: 482095).
- Nucleotide substitutions within the consensus splice site are a relatively common cause of aberrant splic
(PMID: 17576681, 9536098). Algorithms developed to predict the effect of sequence changes on RNA sp
suggest that this variant may disrupt the consensus splice site, but this prediction has not been confirmed
published transcriptional studies.
- In summary, the available evidence is currently insufficient to determine the role of this variant in disease.
Therefore, it has been classified as a Variant of Uncertain Significance.

Methods
- Genomic DNA obtained from the submitted sample is enriched for targeted regions using a hybridization-based protocol, an
sequenced using Illumina technology. Unless otherwise indicated, all targeted regions are sequenced with ≥50x depth or are
supplemented with additional analysis. Reads are aligned to a reference sequence (GRCh37), and sequence changes are iden
interpreted in the context of a single clinically relevant transcript, indicated below. Enrichment and analysis focus on the cod
sequence of the indicated transcripts, 10bp of flanking intronic sequence (20bp for BRCA1/2), and other specific genomic reg

Laboratory Director: [illegible]
Invitae [illegible] San Francisco, CA [illegible]
E: clientservices@invitae.com [illegible]

Name
[illegible]

[redacted] ▸ BRCA ···

Conversation Starter · September 24 ·

Hi sisters!
Weird question but figured someone may know. I'm BRCA2 and wanted to get a token for myself to mark my PBM with the mutation on the front and either "previvor" "mutant strong" or the surgery date or nothing on the back.
Trying to figure out which it is
6174delT
Or... See More

1 · 7 Comments

Like · Comment

View 1 more comment

[redacted] n not sure! But I had a shirt made and did the c. First
Like · Reply · 10w · ❤ 1

[redacted] replied · 1 Reply

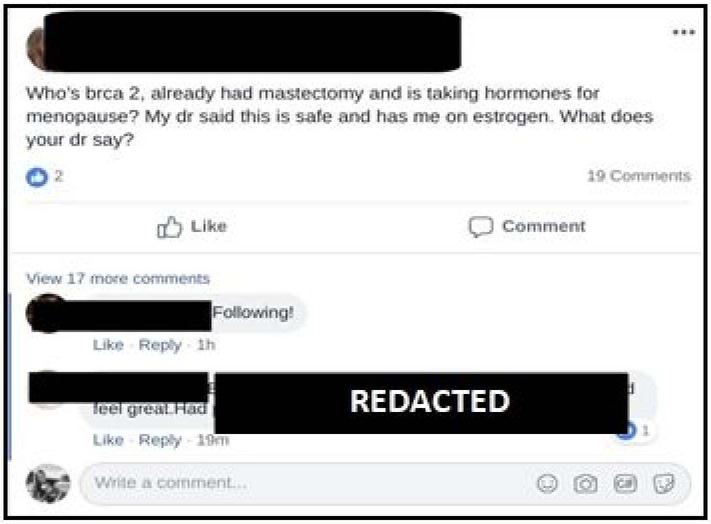
[redacted] would seem that the identifiers.
There have been a couple of different classification systems so that would explain the 2 different numbers.
Like · Reply · 10w

[redacted] replied · 4 Replies

[redacted] 185delAG even though I know the c. classification system is now the standard.
Like · Reply · 10w

[redacted]

Screenshot 3: Questions about health information shared in a Closed Group



[redacted]

Who's brca 2, already had mastectomy and is taking hormones for menopause? My dr said this is safe and has me on estrogen. What does your dr say?

[redacted] Following!

[redacted]

feel great.Had REDACTED

Facebook's leadership knowingly endorsed the Facebook Group product as a PHR

Mark Zuckerberg has demonstrated in multiple public forums that he is aware of and encourages the use of the Groups product for patient care collaborations and coordination.

Zuckerberg and other leaders have repeatedly publicly encouraged and endorsed the use of the Groups product for patient collaborations and care coordination.

These examples were found leveraging the excellent Zuckerberg Files project.

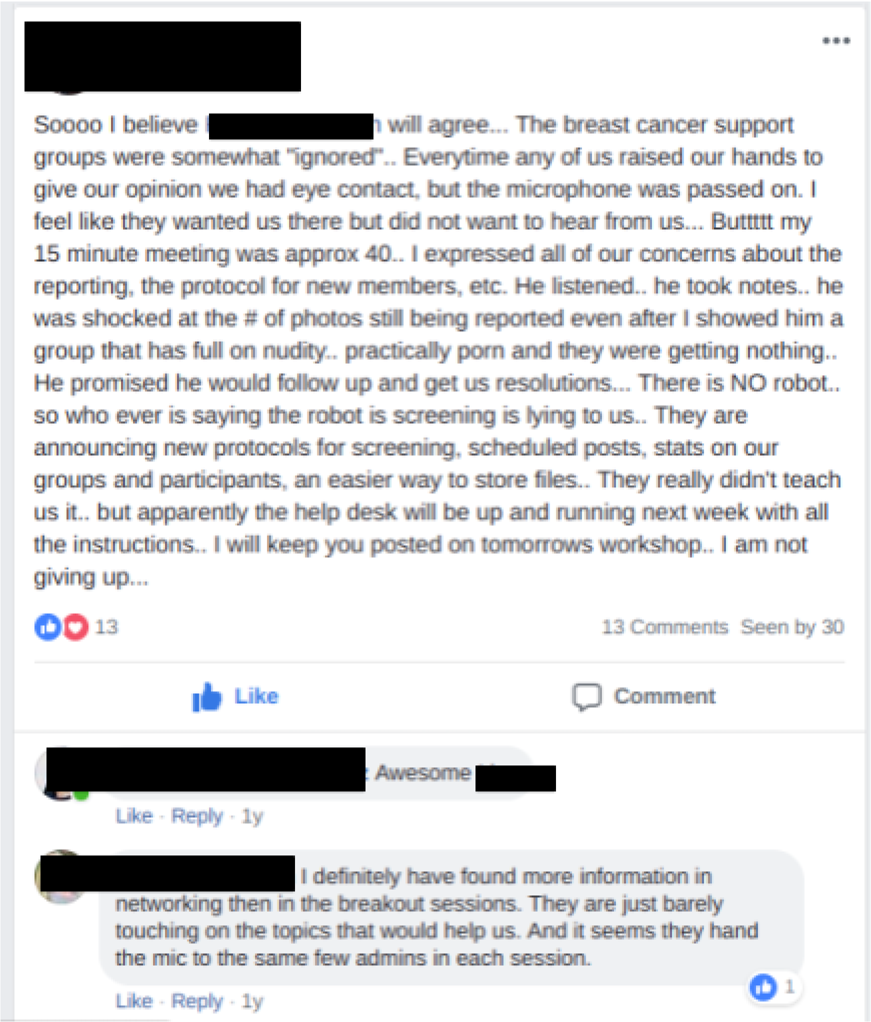
- "People form all kinds of communities. Um, you know, there are more than 700 million people who use groups on Facebook, and a lot of people use it as support groups, um, if people share a health condition." 1-16-2015 Mark Zuckerberg in Colombia. (YouTube link)
- "And there's some pretty amazing stories from folks in our community about how they are coming together, um, for health, uh, reasons. So, whether it's folks who all have an illness in common, um, forming support groups." Townhall Q&A with Mark Zuckerberg from Menlo Park, CA 5-14-2015 (YouTube link)
- "She used Facebook for support during treatment and became a prevention advocate herself." 7-21-2010 500 Million Facebook Stories (Facebook video link)
- Facebook community leader Ana Martinez specifically endorses Facebook support groups as mechanism to treat opioid addiction at an opioid crisis conference in New Mexico. 2-13-2018 Facebook joins effort to fight opioid crisis in New Mexico

Zuckerberg has recently promoted the use of Groups for those with diseases

Mark Zuckerberg has promoted Facebook Groups as a place to find help for “a disease you might have” at the 2018 Facebook Developers Conference. (at about 18:20).

Zuckerberg has heard privacy concerns from users of patient communities

Below we provide screenshots from a Summit in 2017 that convened leaders of cancer Support Groups. At this summit, the Administrator of one of the Closed Support Groups raised concerns about privacy of her own Group, and posted live updates from the summit to share with other Support Group Administrators. This specific Admin participated in a conversation with Mark Zuckerberg where the use of Facebook as PHR by this patient community was clearly discussed.

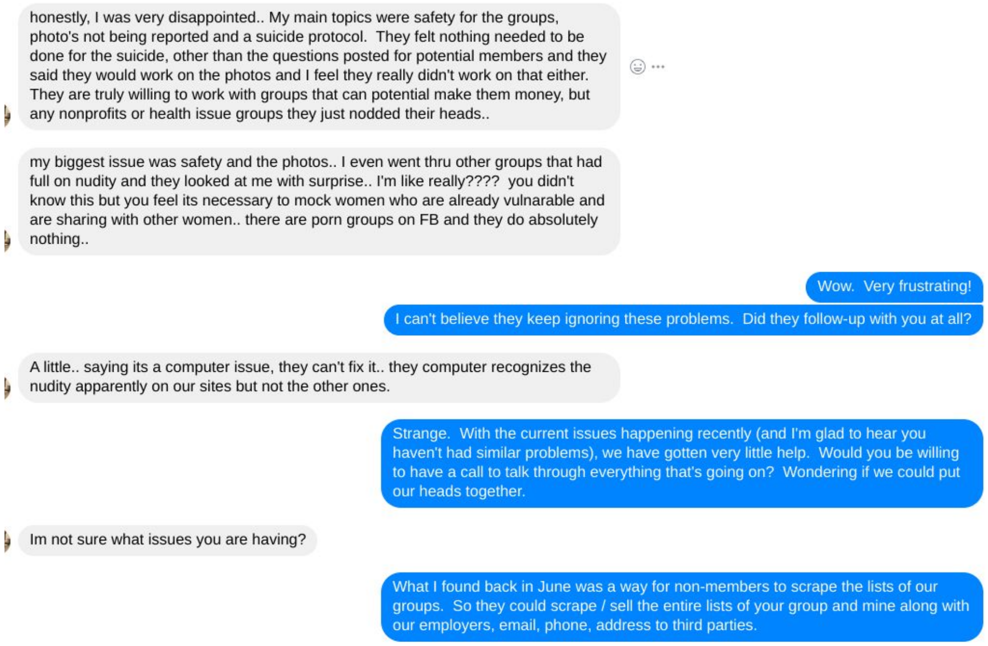


[redacted]

Soooo I believe [redacted] will agree... The breast cancer support groups were somewhat "ignored".. Everytime any of us raised our hands to give our opinion we had eye contact, but the microphone was passed on. I feel like they wanted us there but did not want to hear from us... Buttttt my 15 minute meeting was approx 40.. I expressed all of our concerns about the reporting, the protocol for new members, etc. He listened.. he took notes.. he was shocked at the # of photos still being reported even after I showed him a group that has full on nudity.. practically porn and they were getting nothing.. He promised he would follow up and get us resolutions... There is NO robot.. so who ever is saying the robot is screening is lying to us.. They are announcing new protocols for screening, scheduled posts, stats on our groups and participants, an easier way to store files.. They really didn't teach us it.. but apparently the help desk will be up and running next week with all the instructions.. I will keep you posted on tomorrows workshop.. I am not giving up...

[redacted] Awesome [redacted]

[redacted] I definitely have found more information in networking then in the breakout sessions. They are just barely touching on the topics that would help us. And it seems they hand the mic to the same few admins in each session.



honestly, I was very disappointed.. My main topics were safety for the groups, photo's not being reported and a suicide protocol. They felt nothing needed to be done for the suicide, other than the questions posted for potential members and they said they would work on the photos and I feel they really didn't work on that either. They are truly willing to work with groups that can potential make them money, but any nonprofits or health issue groups they just nodded their heads..

my biggest issue was safety and the photos.. I even went thru other groups that had full on nudity and they looked at me with surprise.. I'm like really???? you didn't know this but you feel its necessary to mock women who are already vulnarable and are sharing with other women.. there are porn groups on FB and they do absolutely nothing..

Wow. Very frustrating!

I can't believe they keep ignoring these problems. Did they follow-up with you at all?

A little.. saying its a computer issue, they can't fix it.. they computer recognizes the nudity apparently on our sites but not the other ones.

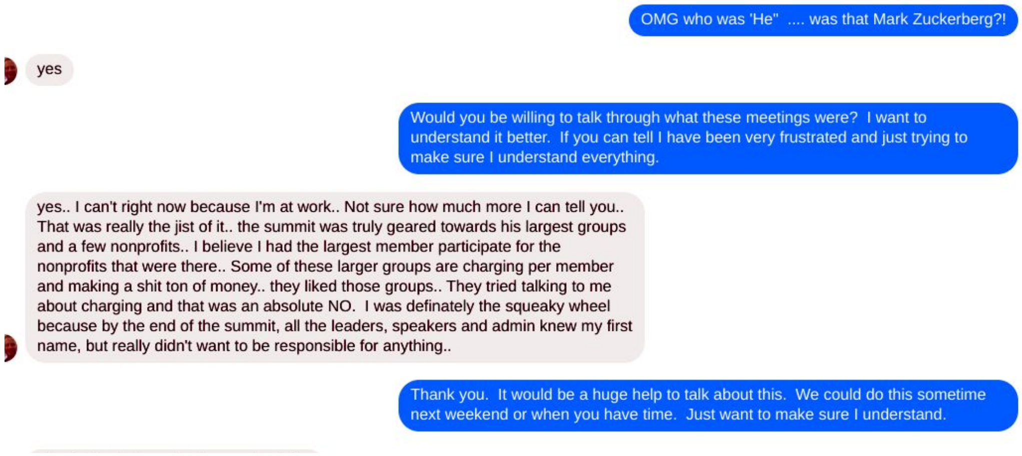
Strange. With the current issues happening recently (and I'm glad to hear you haven't had similar problems), we have gotten very little help. Would you be willing to have a call to talk through everything that's going on? Wondering if we could put our heads together.

Im not sure what issues you are having?

What I found back in June was a way for non-members to scrape the lists of our groups. So they could scrape / sell the entire lists of your group and mine along with our employers, email, phone, address to third parties.

In the conversation above from October 9 2018, a Facebook Administrator of a hereditary cancer Support Group for women undergoing mastectomies was describing her experience at the Group Summit in 2017 with another Administrator.

The conversation continues below where the Administrator describes her meetings where Mark Zuckerberg was present, and where they spoke about the use of Support Groups for health data. This establishes his knowledge of patient Support Groups in 2017.



OMG who was 'He" .... was that Mark Zuckerberg?!

yes

Would you be willing to talk through what these meetings were? I want to understand it better. If you can tell I have been very frustrated and just trying to make sure I understand everything.

yes.. I can't right now because I'm at work.. Not sure how much more I can tell you.. That was really the jist of it.. the summit was truly geared towards his largest groups and a few nonprofits.. I believe I had the largest member participate for the nonprofits that were there.. Some of these larger groups are charging per member and making a shit ton of money.. they liked those groups.. They tried talking to me about charging and that was an absolute NO. I was definately the squeaky wheel because by the end of the summit, all the leaders, speakers and admin knew my first name, but really didn't want to be responsible for anything..

Thank you. It would be a huge help to talk about this. We could do this sometime next weekend or when you have time. Just want to make sure I understand.

Facebook’s privacy and access control sets are inconsistently applied

Recent revelations from documents made public by the UK Government as part of the Six4Three lawsuit show that Facebook has selectively modified its data access deals with certain partners. Those selective data sharing modifications mean that corresponding privacy rules have also been selectively applied by Facebook.

We are unsure of how widespread this is, however we do have evidence that the practice of selectively modifying privacy settings has applied to Groups. The three Group types that Facebook offers are Public, Closed and Secret. The central benefit of a Closed Group over a Secret Group for support communities is that Closed Groups can be found on Facebook’s search.

However, apparently this is a privilege that can be selectively withdrawn from specific healthcare Groups. Kris Pickel of ABC Phoenix reported that a Closed Facebook Group of patients has been removed from Facebook’s search. We have replicated the analysis and it does appear that the Group in question is being censored in the Facebook search results, contrary to policy that Facebook lays out in its Group privacy settings documentation.

Facebook allowed substantial patient health information to leak

There are several major mechanisms by which Facebook has released healthcare information of its users in a manner that, as we describe below, was unfair, deceptive and misleading. Some of these leaks have been resolved by changes that Facebook has recently made to its platform (some changes were made immediately after our complaint was submitted to Facebook). Others continue, but from a user’s perspective, Facebook’s shifting and unclear descriptions of its rules, coupled with how those rules work in real life make the leakages, like the unclear privacy descriptions, unfair and deceptive to consumers.

We have documented two specific mechanisms by which data was leaked.

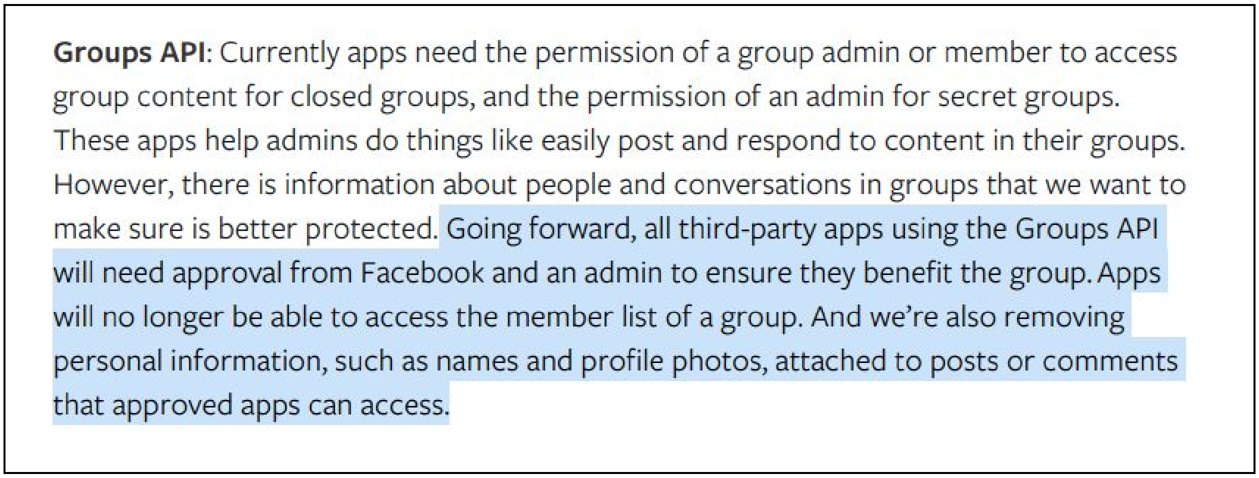
- Exploitation of the Group API
- Exploitation of the Group Privacy Settings

Many of these problems represent cases where user data was shared without their consent. In one case however (Forced SicGRL), user data was shared contrary to consent. To be specific, in at least one case, Facebook users who were informed about the privacy implications of a given “choice,” chose not to share, and then had their data shared despite their choice.

Exploitation of Group API: Leak of PHI

Before Facebook modified its API access in April of 2018, Facebook allowed substantial access to Group related data using its Group API. Before this, even a “mere member” of a Group could allow an App to download substantial clinical data from Closed Groups. Since that change, the Group API became more limited and only available to Group Admins. However, the Apps accessing the API are still confusing and there is still a small risk to clinical Groups that enable Apps.

Figure: Screenshot of Group API Announcement April 4th, 2018

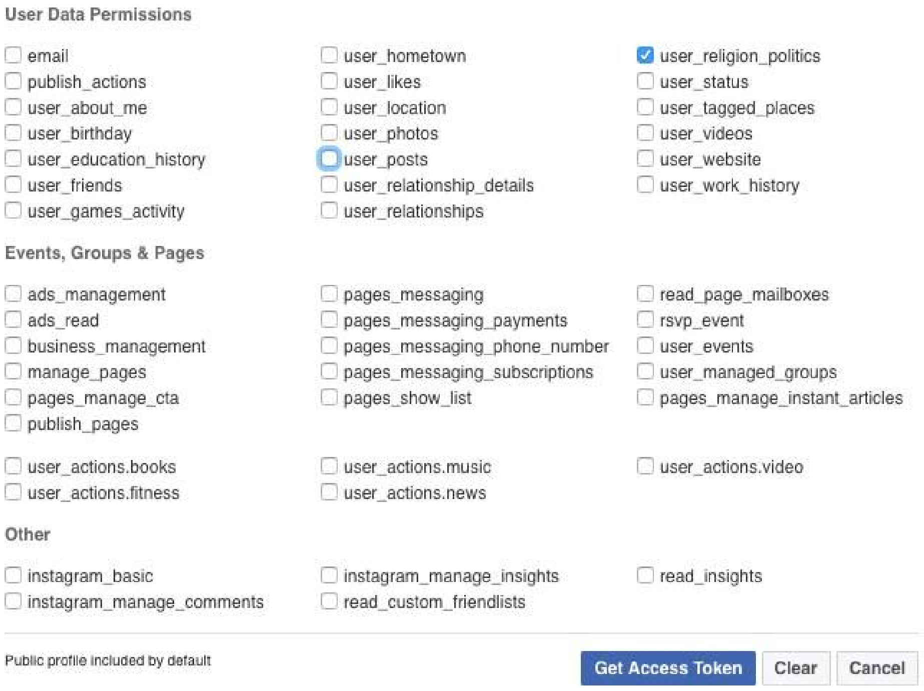


Groups API: Currently apps need the permission of a group admin or member to access group content for closed groups, and the permission of an admin for secret groups. These apps help admins do things like easily post and respond to content in their groups. However, there is information about people and conversations in groups that we want to make sure is better protected. Going forward, all third-party apps using the Groups API will need approval from Facebook and an admin to ensure they benefit the group. Apps will no longer be able to access the member list of a group. And we’re also removing personal information, such as names and profile photos, attached to posts or comments that approved apps can access.

Highlight is ours. When Facebook changed its API, the company stated *“Going forward, all apps will require explicit admin authorization.”* Before this change, any Group user could grant considerable privileges to Apps to read information from a Group that they belonged to.

We are unable to clearly test what types of data access existed previously, however the screenshots that we took before the API change indicate that the data access was considerable.

Figure: Screenshot of Group API Endpoints that were available prior to April 4th, 2018



User Data Permissions

☐ email
☐ publish_actions
☐ user_about_me
☐ user_birthday
☐ user_education_history
☐ user_friends
☐ user_games_activity
☐ user_hometown
☐ user_likes
☐ user_location
☐ user_photos
☐ user_posts
☐ user_relationship_details
☐ user_relationships
☑ user_religion_politics
☐ user_status
☐ user_tagged_places
☐ user_videos
☐ user_website
☐ user_work_history

Events, Groups & Pages

☐ ads_management
☐ ads_read
☐ business_management
☐ manage_pages
☐ pages_manage_cta
☐ publish_pages
☐ pages_messaging
☐ pages_messaging_payments
☐ pages_messaging_phone_number
☐ pages_messaging_subscriptions
☐ pages_show_list
☐ read_page_mailboxes
☐ rsvp_event
☐ user_events
☐ user_managed_groups
☐ pages_manage_instant_articles

☐ user_actions.books
☐ user_actions.fitness
☐ user_actions.music
☐ user_actions.news
☐ user_actions.video

Other

☐ instagram_basic
☐ instagram_manage_comments
☐ instagram_manage_insights
☐ read_custom_friendlists
☐ read_insights

Public profile included by default

This flaw was corrected in the April 2018 API changes. Before this time, however, it was possible for an App developer to make a Group data-mining application, have a Suck Puppet join a given patient Group, and then have that Suck Puppet install the App in order to get real-name coded healthcare data from the Group without Group Administrators' or users' permission. We do not know how often this method was used to download patient data. However, none of these breaches of personal health information or other non-public user information via Group API have been reported to affected users.

Problems with Facebook's Fix:

In the new Group API, Admin users can install third-party Apps that access posts and comments of all users in a Facebook Group, if approved via Facebook's new review process. Those API calls are no longer tagged with the real names of the authors, but they do contain the mention of proper names in post content. Facebook claims that "you cannot see who wrote" posts and comments, but it is possible to have users mention inline in the posts and comments. A fact that is not clearly outlined in the permission screens listed below.

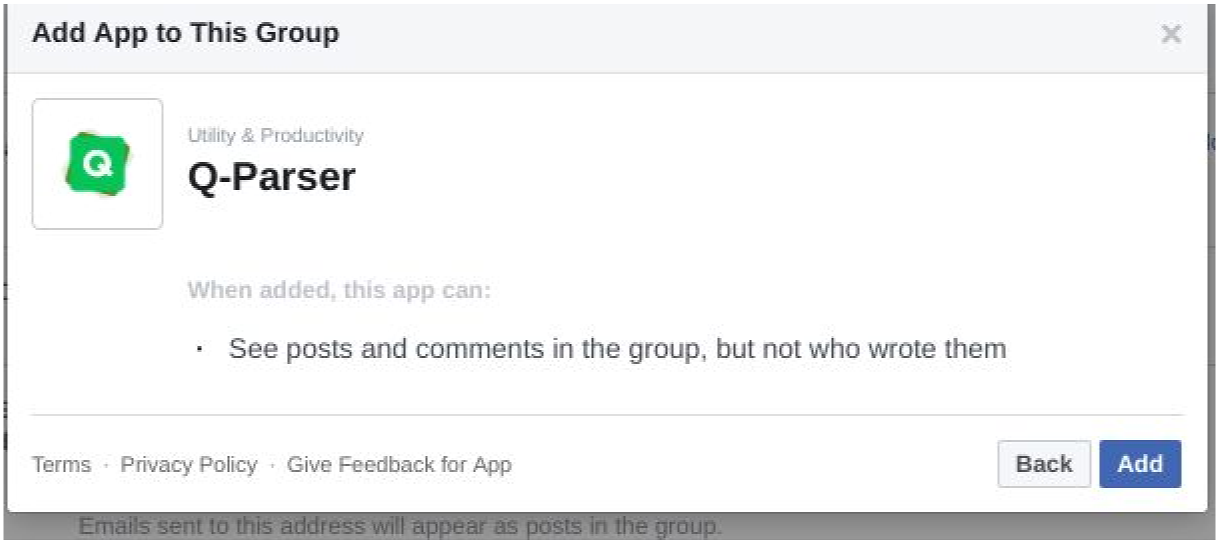
More relevant to these Apps, which still have access to considerable amounts of Group data, is that there is no requirement that the Apps provide details about what they do, or what purpose they serve. While researching these Applications we had to click the "privacy policy" link of the Apps, in order to find the App's domain name, in order to figure out what the Application did.

It is possible for a Group Application to provide information about what the Application does, however, doing so is very rare. It is also not possible to tell what a given App does after it has been installed.

To be specific, we reviewed 30 Group Apps at random, and of these, only 4 had descriptions of what the purpose of the Application was, or any indication of what the App would do with its API access.

Once a Group Application is installed, this information is only available to the Group Administrators. There is no way for Group members to see what Group Apps have been installed on their Group.

Screenshot: Typical Group App Example as of November 2018



Add App to This Group

Utility & Productivity

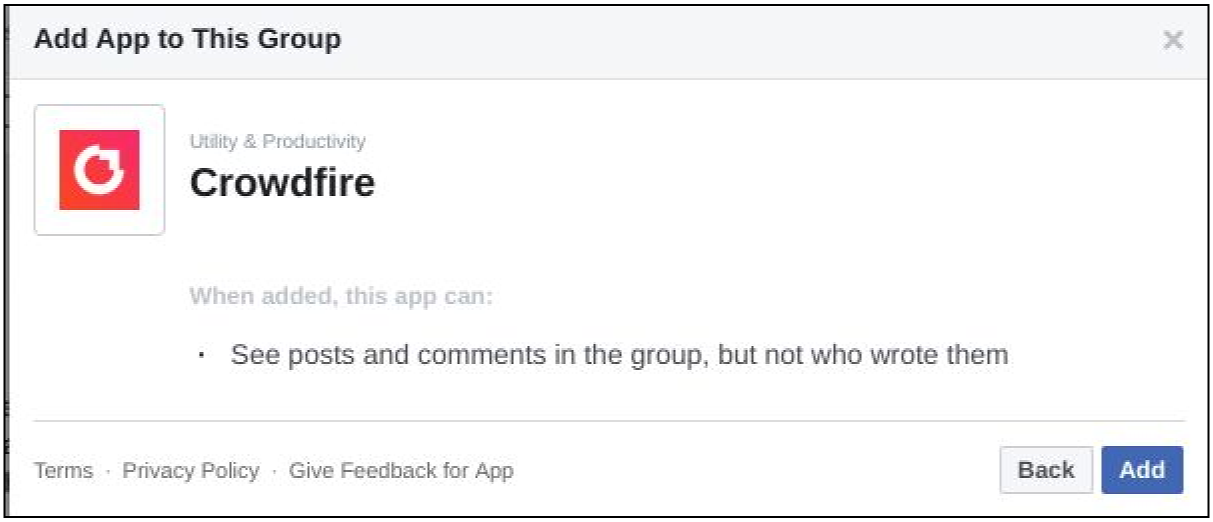
Q-Parser

When added, this app can:

- See posts and comments in the group, but not who wrote them

Terms · Privacy Policy · Give Feedback for App

Emails sent to this address will appear as posts in the group.



Add App to This Group

Utility & Productivity

Crowdfire

When added, this app can:

- See posts and comments in the group, but not who wrote them

Terms · Privacy Policy · Give Feedback for App

Exploitation Methods of Group Privacy Settings: SICGRL Data Leak of PHI

We reported this second flaw to Facebook on May 29, 2018. We refer to this data leak as SICGRL, which is an acronym for “Strict Inclusion Criteria Group Reverse Lookup” Attack.

This flaw allowed any Facebook user to download the membership lists of all Closed Facebook Groups, including patient Groups that have strict inclusion requirements.[2] We submitted a full report of the security vulnerability to Facebook by following their responsible disclosure policy. Yet, Facebook did not publicly announced the change that addressed this issue nor did they acknowledge the data leak.

Our report to Facebook explained the technical details of how Group design flaws potentially exposed the private health information of millions of Facebook users. All Closed Groups on Facebook were impacted by these problems.

The official position from Facebook in response to this report was that there was not a “privacy loophole” or a “security vulnerability” at all. Specifically, Facebook’s security team responded to the technical report as follows:

> *.....some people may have legitimate reasons to want to create groups which have different feature-sets than the functionality we provide today. We would like to provide as many people as possible with a way to use Groups to serve their needs. However, we can not guarantee that our Groups product will always have the exact feature-set that people want. A lack of such functionality may be disappointing for people and limit certain usage of Facebook, but we do not consider it to be a privacy or security concern in the product.*[3]

This carefully written reply essentially boils down to the position of “Facebook’s Group product does not have the privacy features needed for clinical Support Groups, and should not be used for that purpose”. However, it is so obliquely phrased that we are unable to take this back to the admins of Clinical Groups to convince them that they should leave Facebook.

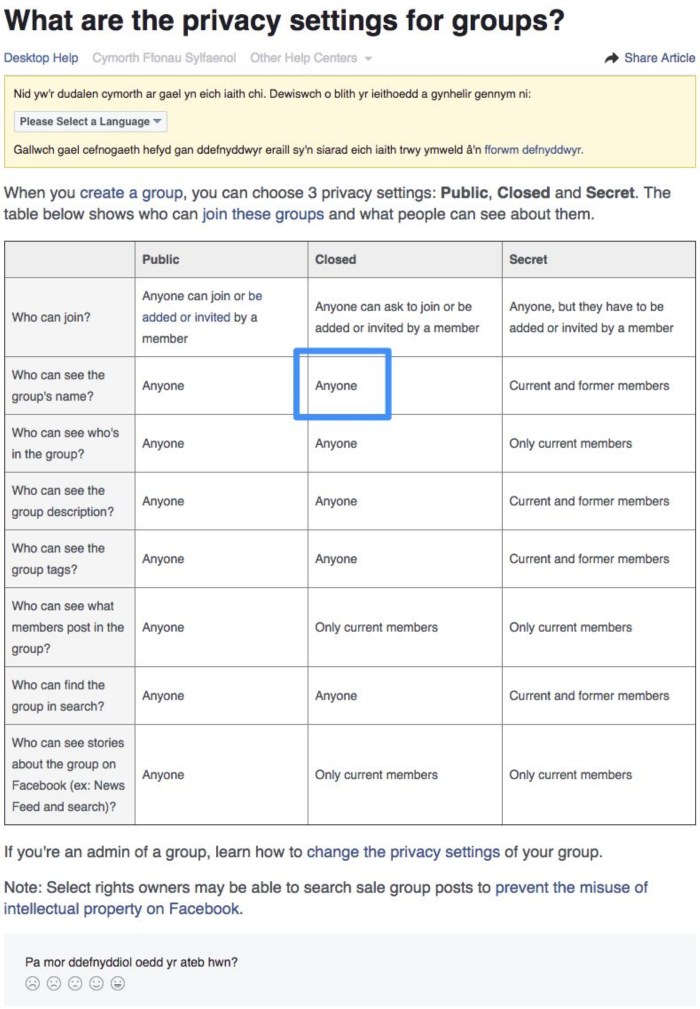
[2] For the purpose of this document, we define “strict inclusion requirements” as a screening practice by administrators to add members with a specific health condition such as HIV Positive, BRCA Positive, Sexual Assault Survivor, etc.

[3] This is cited from the response from Facebook’s security team after submitting a 30-page report on Facebook’s design flaws via their White Hat Portal on May 29, 2018.

News Headlines About SICGRL in July 2018

Articles describing various aspects of this enormous privacy vulnerability and subsequent UI change were reported CNBC, Forbes, Fortune, The Verge, Venturebeat, and many other outlets in July 2018. [4] [5] [6] [7]

Screenshot: Facebook Group Privacy Settings BEFORE July 2018



What are the privacy settings for groups?

Nid yw'r dudalen cymorth ar gael yn eich iaith chi. Dewiswch o blith yr ieithoedd a gynhelir gennym ni:

Gallwch gael cefnogaeth hefyd gan ddefnyddwyr eraill sy'n siarad eich iaith trwy ymweld â'n fforwm defnyddwyr.

When you create a group, you can choose 3 privacy settings: **Public**, **Closed** and **Secret**. The table below shows who can join these groups and what people can see about them.

	Public	Closed	Secret
Who can join?	Anyone can join or be added or invited by a member	Anyone can ask to join or be added or invited by a member	Anyone, but they have to be added or invited by a member
Who can see the group's name?	Anyone	Anyone	Current and former members
Who can see who's in the group?	Anyone	Anyone	Only current members
Who can see the group description?	Anyone	Anyone	Current and former members
Who can see the group tags?	Anyone	Anyone	Current and former members
Who can see what members post in the group?	Anyone	Only current members	Only current members
Who can find the group in search?	Anyone	Anyone	Current and former members
Who can see stories about the group on Facebook (ex: News Feed and search)?	Anyone	Only current members	Only current members

If you're an admin of a group, learn how to change the privacy settings of your group.

Note: Select rights owners may be able to search sale group posts to prevent the misuse of intellectual property on Facebook.

Pa mor ddefnyddiol oedd yr ateb hwn?

☹ ☹ ☺ ☺ ☺

The blue box highlights the settings for emphasis. You can see the previous (BEFORE) version of the Facebook Group privacy settings here on wayback machine. The current (AFTER) page

[4] Facebook Violates Trust of 'Private' Patient Groups

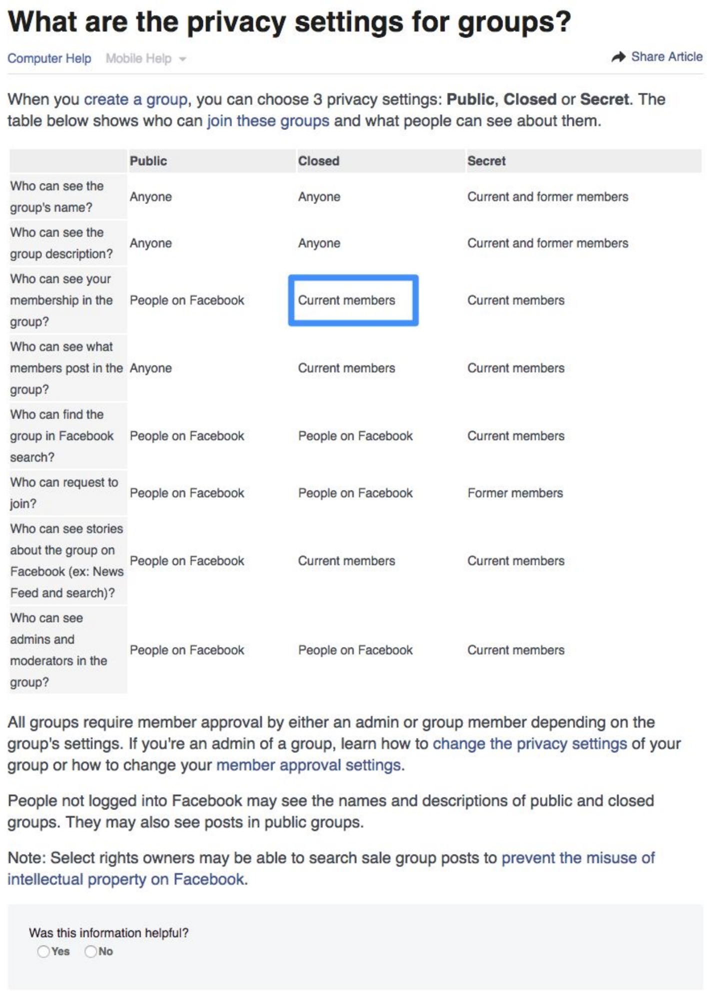
[5] Facebook Closes Loophole That Revealed Personal Data of People in 'Closed' Groups

[6] Facebook changes privacy settings after outing members of a closed medical Support Group

[7] Marketers could harvest member data from closed Facebook Groups as recently as June, report says

that illustrates the current Facebook Group privacy settings is here, and looks like the screenshot below

Screenshot: Facebook Group Privacy Settings AFTER July 2018



What are the privacy settings for groups?

When you create a group, you can choose 3 privacy settings: **Public**, **Closed** or **Secret**. The table below shows who can join these groups and what people can see about them.

	Public	Closed	Secret
Who can see the group's name?	Anyone	Anyone	Current and former members
Who can see the group description?	Anyone	Anyone	Current and former members
Who can see your membership in the group?	People on Facebook	Current members	Current members
Who can see what members post in the group?	Anyone	Current members	Current members
Who can find the group in Facebook search?	People on Facebook	People on Facebook	Current members
Who can request to join?	People on Facebook	People on Facebook	Former members
Who can see stories about the group on Facebook (ex: News Feed and search)?	People on Facebook	Current members	Current members
Who can see admins and moderators in the group?	People on Facebook	People on Facebook	Current members

All groups require member approval by either an admin or group member depending on the group's settings. If you're an admin of a group, learn how to change the privacy settings of your group or how to change your member approval settings.

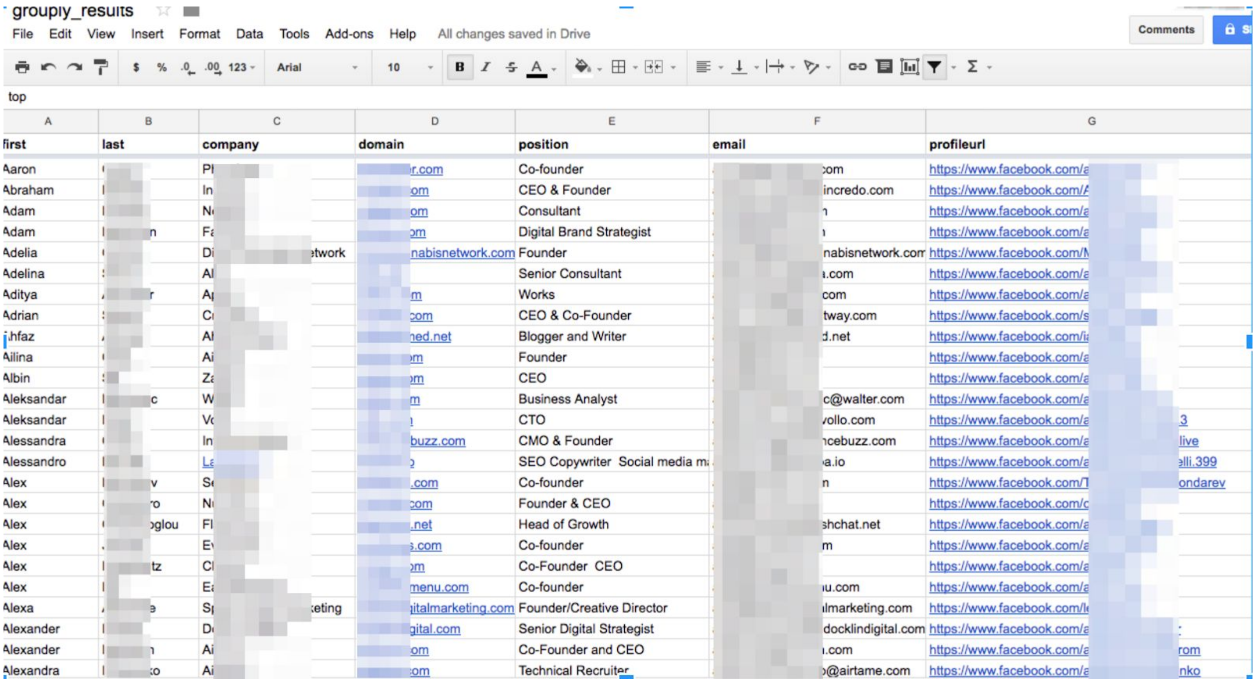
People not logged into Facebook may see the names and descriptions of public and closed groups. They may also see posts in public groups.

Note: Select rights owners may be able to search sale group posts to prevent the misuse of intellectual property on Facebook.

Was this information helpful?
○ Yes ○ No

How These Privacy Settings Enabled SICGRL List Scraping of PHI En Masse Before July 2018

Before these changes to security settings, any Facebook user was able to download the entire membership list from all ‘closed’ Facebook Groups. These lists included the real names of each Facebook User, sometimes (depending on the users settings) the city location of the user, and the link to their Facebook profile.[8]


groupiy_results
File Edit View Insert Format Data Tools Add-ons Help
All changes saved in Drive
Comments
$ % .0 .00 123
Arial
10
B I S A
Σ
top
A B C D E F G

first	last	company	domain	position	email	profileurl
Aaron	[redacted]	Pl[redacted]	[redacted]r.com	Co-founder	[redacted]com	https://www.facebook.com/a[redacted]
Abraham	[redacted]	In[redacted]	[redacted]om	CEO & Founder	[redacted]incredo.com	https://www.facebook.com/A[redacted]
Adam	[redacted]	N[redacted]	[redacted]om	Consultant	[redacted]n	https://www.facebook.com/a[redacted]
Adam	[redacted]n	Fa[redacted]	[redacted]om	Digital Brand Strategist	[redacted]n	https://www.facebook.com/a[redacted]
Adelia	[redacted]	Di[redacted]etwork	[redacted]nabisnetwork.com	Founder	[redacted]nabisnetwork.com	https://www.facebook.com/N[redacted]
Adelina	[redacted]	Al[redacted]	[redacted]	Senior Consultant	[redacted].com	https://www.facebook.com/a[redacted]
Aditya	[redacted]r	Ap[redacted]	[redacted]m	Works	[redacted]com	https://www.facebook.com/a[redacted]
Adrian	[redacted]	C[redacted]	[redacted]com	CEO & Co-Founder	[redacted]tway.com	https://www.facebook.com/s[redacted]
hfaz	[redacted]	Al[redacted]	[redacted]ned.net	Blogger and Writer	[redacted]d.net	https://www.facebook.com/i[redacted]
Ailina	[redacted]	Ai[redacted]	[redacted]om	Founder	[redacted]	https://www.facebook.com/a[redacted]
Albin	[redacted]	Za[redacted]	[redacted]om	CEO	[redacted]	https://www.facebook.com/a[redacted]
Aleksandar	[redacted]c	W[redacted]	[redacted]m	Business Analyst	[redacted]c@walter.com	https://www.facebook.com/a[redacted]
Aleksandar	[redacted]	Vo[redacted]	[redacted]	CTO	[redacted]vollo.com	https://www.facebook.com/a[redacted]3
Alessandra	[redacted]	In[redacted]	[redacted]buzz.com	CMO & Founder	[redacted]ncebuzz.com	https://www.facebook.com/a[redacted]live
Alessandro	[redacted]	La[redacted]	[redacted]o	SEO Copywriter Social media m	[redacted]a.io	https://www.facebook.com/a[redacted]elli.399
Alex	[redacted]v	Se[redacted]	[redacted].com	Co-founder	[redacted]n	https://www.facebook.com/T[redacted]ondarev
Alex	[redacted]ro	N[redacted]	[redacted]com	Founder & CEO	[redacted]	https://www.facebook.com/c[redacted]
Alex	[redacted]oglou	Fl[redacted]	[redacted].net	Head of Growth	[redacted]shchat.net	https://www.facebook.com/a[redacted]
Alex	[redacted]	Ev[redacted]	[redacted]s.com	Co-founder	[redacted]m	https://www.facebook.com/a[redacted]
Alex	[redacted]tz	Cl[redacted]	[redacted]om	Co-Founder CEO	[redacted]	https://www.facebook.com/a[redacted]
Alex	[redacted]	Ea[redacted]	[redacted]menu.com	Co-founder	[redacted]u.com	https://www.facebook.com/a[redacted]
Alexa	[redacted]e	Sp[redacted]keting	[redacted]italmarketing.com	Founder/Creative Director	[redacted]lmarketing.com	https://www.facebook.com/l[redacted]
Alexander	[redacted]	D[redacted]	[redacted]gital.com	Senior Digital Strategist	[redacted]docklindigital.com	https://www.facebook.com/a[redacted]
Alexander	[redacted]n	Ai[redacted]	[redacted]om	Co-Founder and CEO	[redacted].com	https://www.facebook.com/a[redacted]rom
Alexandra	[redacted]ko	Ai[redacted]	[redacted]om	Technical Recruiter	[redacted]o@airtame.com	https://www.facebook.com/a[redacted]nko

While investigating how the Grouply.io tool worked, we realized the underlying problem was in the design of the privacy controls themselves. Facebook had simply not accounted for the fact that when a Closed support Group had a strict inclusion requirement, (i.e., you must have HIV, or you must have a particular BRCA gene) that membership in the Group reflected specific health information of the Group members. This problem applied to any strict inclusion requirement. For instance, a user who joined a “redheads only” Group, would be communicating to the world that they had red hair. The problem was dangerous for Groups whose inclusion requirements communicated some specific personal vulnerability about its members to the public.

[8] We discovered this problem through use of a Chrome browser extension called Grouply.io. This tool, which has since been taken down, (presumably by Facebook's lawyers) allowed anyone to download the contents of any Facebook Group as a CSV file.

For instance, if the inclusion requirement in a Group was “being in a religious minority in a certain country” or “being homosexual in a country where homosexuality is a capital offense”, then the fact that membership in the Group was public information meant that these users could be targeted. These vulnerable users were often presented with two distinct privacy messages- one saying their membership was public (from Facebook) and one saying the membership in the Group was private (from the Group Administrators).

It is possible that some of the Facebook-borne genocides have taken advantage of this flaw. It is also possible that a variation of the problem, where a rogue user creates a “honeypot” Group for a particular vulnerable population, and then mines the Group membership list for vulnerable individuals is also being leveraged to expose Facebook users to life-threatening privacy violations. Obviously, when a person is threatened due to participating in a Facebook Group, the Groups are not “safe” as each participating user had assumed.

It is not obvious to users who joined these “Closed” Groups that their membership status in those Groups is available to download. Almost all online communities allow users to “lurk”, meaning that they can join a community and listen, but their presence will not be made known to the other participants in the Group until they choose to ‘out’ themselves by saying something. Many of those who have joined Facebook Groups that were advertised as “safe” or “private” likely still believe that their participation in the Groups remains private.

Facebook encourages the idea that it is possible to “lurk” in Groups by providing tools that allow users to control which “Public” Groups will be displayed on a user’s “About” page. This gives the sense that the only mechanisms by which User A can discover which Groups user B is a member of is for User A to go visit the page of User B. All Closed Groups are automatically hidden on a user’s “About” page. This contributes to the notion that mere participation in “Closed” Groups is not information that is readily available.

In order for a user to properly mentally model whether they are able to “lurk” they must understand the basic concepts of a “Reverse Lookup Attack”, or a “Gray Pages Attack” (from the notion of a reverse lookup telephone directory). So, when a given User A looks at User B’s public page, and sees no membership information for a Group that A knows that B is actually a member of (because it is a Closed Group), A then assumes that their own information is private. But A does not understand that even if B cannot see A’s information, C, who has downloaded the membership lists for dozens or hundreds of Groups, knows virtually all of the Groups that User A and User B are a member of. Facebook users have no idea that a “gray page” reverse lookup tool continues to be trivial to create by any technically competent Facebook user. As a result, they have no idea that their membership in “Diabetes-only” Facebook Groups is essentially public information.

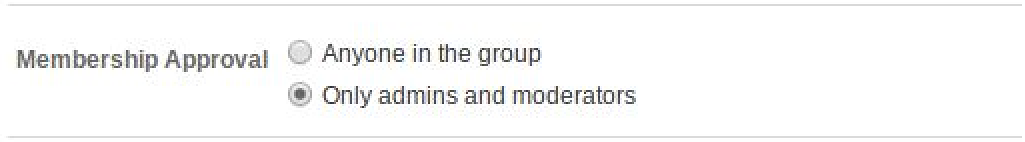
Problems with Facebook's ‘fix’:

While it is no longer possible for non-Group-members to download the member lists from thousands of Closed Groups and millions of users in a single attack, it is still possible to download the member list if you are a member of the Group. We have seen some evidence in an uptick in ‘fake membership applications’ to a small sample of Closed clinical Groups. We believe that this could be the response of malicious actors who are now using Suck Puppet accounts that previously had generous access to Closed Group membership data, that are now seeking to restore their access.

Therefore while the most dangerous permutation of this problem has been corrected, the underlying problem is still operating today. People join Facebook Closed Support Groups presuming that they can lurk, and that they are protected from dangerous data sharing by their silence. But instead, the “membership” information is being broadcast in a way that is very simple for a Suck Puppet to acquire, making the Groups unsafe despite Facebook’s statements to the contrary.

Forced SicGRL, forced data sharing against user consent

It is possible for one user on Facebook to add another user to a Group. The ability to “force-add” is somewhat controlled by the following Group Admin setting:



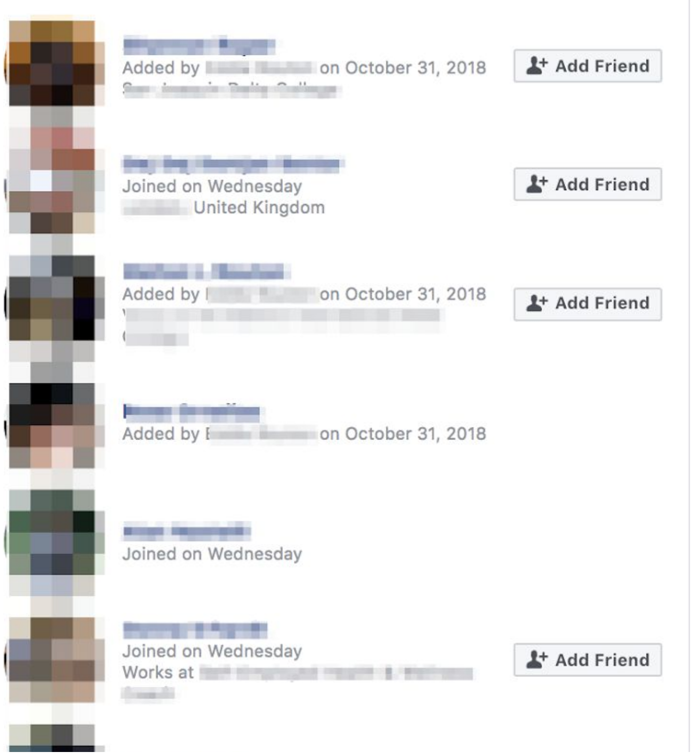
Membership Approval ○ Anyone in the group
● Only admins and moderators

The most problematic permutation of the SicGRL data leak is derived from this “force add” functionality. There are two cases where this can occur, one of which is not merely a “without consent” event, but an “against consent” event.

- The first permutation is when User A has a “Facebook Friends” relationship with User B, and knows some personal fact about them, e.g., “they are a member of a local Republican party” or “that user is HIV positive.” And User A is a member of some Group Y with an explicit inclusion requirement (e.g., only for Republicans or only for people with HIV, respectively). User A can simply “add” User B to the Group. Doing this initiates an approval process from the Group Administrator, but frequently the fact that User A is “vouching” for User B’s inclusion status is enough to dissuade the Group Admin from even checking whether User B would like to be in the Group. Once the Group Administrator has approved User B, User B will receive a message from Facebook indicating that they have been added, and to “click here” if they do not want to be in the Group.

- The second permutation is far more problematic. This version does not involve a “friend” at all. Instead, User C visits Group X (again, a Closed Group with an inclusion requirement that is an indication of a vulnerable status of some kind), and reads the disclaimers. User C reads all of the relevant privacy messages, both on and off the Group, and decides that they are not comfortable having their vulnerable information exposed by being a member of Group X. As a result, User C cancels their application process, and leaves the Group signup page entirely, to visit something else on the Internet. In this case, the User C has clearly expressed “I see what joining this Group means, and I do not want that”. Despite this, the Group Admin of Group X sees that the application has been clicked to join the Group, but that the questions have not been answered. In response, the Group Admin simply adds User C to the Group in question, using their ability to force-add users. As in the previous case, User C would receive a message indicating that they had been added to the Group, contrary to their expressed preference.

Once a user has been added to a Group, they appear differently in the membership view. They appear with a tag line “Added by X” rather than “Joined”. The screenshot below is from a political Group on Facebook where many of the participants were added, rather than intentionally joining.



[redacted]
Added by [redacted] on October 31, 2018
[redacted]

[redacted]
Joined on Wednesday
[redacted] United Kingdom

[redacted]
Added by [redacted] on October 31, 2018
[redacted]

[redacted]
Added by [redacted] on October 31, 2018

[redacted]
Joined on Wednesday

[redacted]
Joined on Wednesday
Works at [redacted]

In the June 20th, 2018 response to our report to Facebook, Facebook confirmed that the above description is an accurate reflection of how the platform functions, but concluded that “*we do not consider it to be a security or privacy concern in the product*”.

Facebook selectively enforces its real-name policy

Facebook is famous and unique for its real-name policy. Because the policy is poorly enforced, many advanced users, including Group Administrators, choose to use protective fake names. Frequently, Groups with sensitive strict inclusion requirements specifically recommend that other users protect themselves by violating Facebook's Real Name policy.

However, the policy is not so lax that casual users can easily create a fake-name account. Facebook's signup process is highly reliant on the validation from friend connections. Accounts that have no friends, and are from email addresses that Facebook has not already seen in others' contact lists, are much more likely to be challenged during signup.

This partial enforcement creates an environment where Suck Puppet masters, who have the time and energy to create complex fake accounts that are able to fool the Facebook sign-up process, are able to create many Suck Puppets for the purpose of data mining other users. While legitimate users are forced to use their real names, putting them at greater risk to data leaks.

Facebook recognizes that in some cases, users on its platform need to have name privacy. For example, in the Facebook dating app, only your first name is exposed to potential dates.

Our submission to Facebook suggested that Facebook modify only "support" Group types to have a similar name privacy layer, and Facebook did not respond to this suggestion.

Active exploitation of these privacy problems

Cat Ferguson at The Verge wrote Predatory Behavior Runs Rampant In Facebook's Addiction Support Groups. In this report, Ferguson details Facebook users who were contacted via Facebook messages and offered addiction treatments that were not legitimate. These users were contacted because they signed up for a Facebook Group for addiction support, either for themselves or for a loved one. We believe that SicGRL was the mechanism by which the salespeople for these fraudulent treatment programs found their victims.

It is also likely that regimes who have used Facebook to target repressed Groups of individuals with death squads and other violence have been using the types of Facebook Group leaks that we are detailing here in order to make determinations on who to target for harm. The best resource for context of the use of Facebook for targeting violence is the Frontline Facebook Dilemma series.

Arguments

In the facts section, we did our best to only discuss the provable facts about the way that the Facebook Groups product works, and how this has impacted the patient communities that use the product. In this section we will detail our arguments about what these facts mean, as well as what the FTC should do as a result of them.

Facebook deceptively lures vulnerable users into joining unsafe clinical Support Groups.

Facebook offers the illusion of control but ignores and obscures privacy decisions.

The Facebook line that users can “control what others see” in Closed and Secret Groups is deceptive. It is true only in the narrowest sense, and even a cursory review of their data policy makes it clear that using Facebook is effectively a game of privacy roulette in which users are unable to know in advance which “connections” will hurt them by downloading the data from posts in Closed and Secret Groups. Despite this, Facebook uses the language of “safety” and/or “control” prolifically in interviews, in testimony and even in TV ads. This entire approach is deceptive, given that Facebook frequently uses the “sense of control” that it provides against users as a key bonus for joining the platform, which in turn ensures platform growth.

To understand whether Facebook’s assertions of safety are correct, a Facebook user must successfully model all of the implications of a complex and arbitrarily enforced privacy design (e.g. understanding the threat of a reverse lookup, in the context of three different types of Groups, and the possibility that Facebook might not be honoring those policies for *this* Group), in order to correctly calculate whether their information can be downloaded by strangers. The very fact that it took us nearly 40 pages to explain this to the FTC tells you that an ordinary consumer cannot effectively do this testing and that Facebook’s disclosures to users through terms of use and privacy policies are ineffective and deceptive. Indeed, Facebook’s materials made available to users and potential users create user expectations that they are in control. Requiring users to personally assess the privacy calculus of a reverse lookup attack potential is deceptive, unfair and misleading.

This is not entirely without precedent. Phone companies used to create “gray pages” that were only available to trusted insiders and, eventually, Suck Puppets. Most telephone users remain unaware that gray pages ever existed, or that they were ever used for social engineering purposes.

Facebook's selectively-enforced real name policy unfairly impacts vulnerable people and serves to deceive users into thinking that other users are legitimate.

Forcing only some users to use their real names places greater risks on the already vulnerable. Facebook places honest users in the position where they have to use their real name in order to use the service at all, even if they do not want to. However, Facebook does not insist that everyone use their real name and some sophisticated users, including Suck Puppets, are able to circumvent this requirement. This is unfair and misleading to those users who presume that everyone has had to follow the same rules that they did. Presumably, users who assume that Facebook enforces its real name rules may be more likely to fall victim to joining a Group that has been set up as a honeypot, by a Suck Puppet. Similarly, all other members of a legitimate support Group look equally plausible, despite the fact that some of them are Suck Puppets who exist only to download their interactions with a Group labeled as "safe" and/or "private" by Group Administrators.

This problem is substantially compounded by the fact that Facebook has clearly recognized that name privacy is vital for a **new** product. As we documented in the facts, Facebook only uses first names in its new dating application. The implication here is that old products, that serve the engagement and data mining needs of its profit model, are not worth reengineering to ensure privacy. This is exactly the problem that Sandy Parakilas represented as happening in his tenure at Facebook in 2011 and 2012. It could be argued, if we were the first parties to make these types of arguments to Facebook, that these problems were unintentional. Given that Facebook employees were obviously protesting these issues as far back as 2012 means that Facebook knew of the problems but did nothing to correct them, which is active deception.

Facebook abuses trust in the patient community in order to create a profitable product.

Groups provide Facebook users with a mechanism of engagement around sharing of personal health information that is exclusive to Facebook. The original appeal of joining Facebook, for many users, was to connect with people they already knew in the real world. By developing the Groups product, and expending tremendous ongoing efforts to ensure that members are participating in Groups, Facebook ensures that its users are exposed to other users who profoundly resonate with them, not because of real-world proximity, but because of shared values or shared experience and, more importantly, because of shared vulnerabilities, trauma or disease. Facebook's priority here must be calculated in terms of the relative level of exposure to Groups products vs advertisements. It is obvious that Facebook places a multi-billion dollar valuation on ensuring that its users are in Groups.

Having relationships that were created through a profoundly emotional shared experience and available only through Facebook ensures that users have a connection that they cannot find anywhere else. This is a feature that real-world coffee shops and bars cannot match. As a result of this dynamic, patients have flocked to Facebook, and then once they realized the privacy implications of being on Facebook, have consistently begged to be made safe. Instead, Facebook has given a feature that they have begged for to an unrelated, and relatively trivial product that has not yet launched. The fact that privacy features that can be developed for other products, but are being denied to patient communities is deceptive. The fact that the feature is available elsewhere is unfair. The fact that working privacy features are withheld, while the current privacy architecture is clearly broken is unfair, deceptive and misleading.

Facebook has co-opted well-meaning Group Administrators to deceive Facebook users regarding the status of their privacy. Sampling patient and other vulnerable Group descriptions reveals that even Group Administrators, who are likely Facebook's most sophisticated users, have misconceptions regarding how Facebook privacy controls work. What is worse, these Group Administrators spread this misinformation to their users in a manner that ensures that end users cannot tell the difference between the privacy representations that are made by Facebook and those that are made by the Group Administrators. The result is that for a typical patient user of Facebook, the sum of what they have been told regarding the privacy of their patient community when they made the choice whether to join, was not at all reflective of the actual data sharing mechanisms governing their data on the Groups platform. This is deceptive, misleading and unfair.

These problems are not hard for Facebook to fix

It would be trivially easy for Facebook to correct this problem. Facebook can easily determine which Groups are established for, and which attract, populations of vulnerable people. It could do this by analyzing the text of descriptions or just by reviewing all "Support" Groups. Facebook could write machine learning algorithms to detect when Group admins had communicated incorrect privacy information, ensuring that they could quickly be corrected. However, it would not actually take that much time to review the information manually. In the scheme of things, there are not that many Groups where this matters, even considering the number of different languages that Facebook supports.

Once these "conflicting privacy statements" were corrected, Facebook could require the respective Group Administrators to correct the ongoing miscommunication, and could communicate to Group members the correct privacy information.

Facebook could easily solve the problem of conflicting privacy statements, with a week's worth of focused work. But it has chosen not do that, months after we informed them, carefully, about these and other privacy problems at Facebook. While we may have been the first to reveal that this specific problem was being exploited in the wild (as evidenced by the Verge article), we are certainly not the first patients to bring issues like this to Facebook's attention. Why hasn't

Facebook fixed this specific issue, given their new focus on privacy and safety? Why didn't they acknowledge the issue in their response to us?

Facebook could also easily fix the name-privacy issue. They could likely do this in a way that does not lower the community engagement or "stickiness". They could have prevented "Group member" download of member lists, in only "Support" Groups. Or they could have made it an option that Group admins could choose, to increase the privacy of very specific Groups. Or they could have made it an option that a user could specifically choose in the settings. Why did they not make any of these changes or even respond to suggestions that they consider these options?

The only reasonable explanation is that the organization is fundamentally incapable of re-examining the fundamental privacy design of its platform -- as a management matter, not as a technical matter. Even as it is constructively and narrowly criticized, and shown to be hurting users, "sacred" design decisions cannot be reconsidered. Even when they are obviously flawed to anyone except the high-level Facebook leadership that continues to insist on them.

Facebook pushes the philosophy that Control is privacy, which would be fine if Facebook were actually providing it's users with meaningful control. Instead they are providing the 'user experience of control,' which is then ignored, and labeling the sense of safety that resulted from that 'user experience' as 'privacy,' while actually allowing for the undermining of user expectations about their privacy choices.

"Control as privacy" is an illusion when the consequences of privacy decisions are impossible to correctly calculate. Facebook has been informed about how Groups confuse the privacy representations, and has not taken simple and easy steps to fix that problem. Facebook relies on consumer confusion about its privacy settings as a business asset. It leverages the confusion to generate the kinds of user details that it needs to target ads, and to create the kind of exclusive social connections that make its platform "sticky" to users. Facebook profits from the confusion that it creates about user privacy and externalizes the harm associated with this confusion to individual users. In short, the downside of Facebook is made to be exclusively the problem of the Facebook user. Specifically, a problem that is deceptive, unfair and misleading.

Facebook ignores important privacy choices

Frankly, the second permutation of the force-add feature -- “force-add-against-consent” -- deserves its own category in this complaint. The force-add functionality is, quite simply, an engine for circumventing any given user’s aversion to participating in the Facebook Groups product. There is no other part of our compliant that better highlights the explicit “betray privacy to ensure growth” strategy that lies at the heart of all of the privacy design flaws that we illustrate. Users who had their consent contradicted were exposed to dozens of privacy-related issues, only a few of which we discuss carefully here. All of this, after users explicitly refuse to take the specific risk. This is deceptive, unfair and misleading to consumers. This illustrates a greed-inspired malevolence, rather than mere confusion or incompetence.

Facebook’s platform is a PHR. After we notified the company of a breach, they did not notify others, violating the FTC Health Breach Notification rule.

According to the definitions set forward by the FTC, Facebook is clearly a PHR. It is obviously being used in this manner, as we document in *“Facebook’s Groups product is used as a Personal Health Record.”*

FTC guidance explains when a business becomes a vendor of PHRs subject to the FTC rule:

> *For the purposes of the Rule, your business is a vendor of personal health records if it “offers or maintains a personal health record.” A personal health record is defined as an electronic record of “identifiable health information on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual.”* ***For example, if you have an online service that allows consumers to store and organize medical information from many sources in one online location, you’re a vendor of personal health records.***

The emphasis is ours. Given that all information on Facebook is identifiable (due to the Real Name Policy discussed above), the only question is whether the information is health information and whether it is controlled by or for the individual. Whether it is drawn from several sources is not critical to the definition because it says “can be drawn” rather than “must be drawn”, but the Facebook platform certainly meets that portion of the definition too.

Patients use the Facebook Groups platform to connect with patients, providers, insurance companies, medication companies and researchers, specifically to discuss healthcare concerns.

However, people upload their healthcare data to Google Drive spreadsheets, or to blogging platforms like Medium or Tumblr. People use Microsoft’s Office 365 documents as patient logs, or use Amazon AWS databases to track data from their home-grown medical devices. People use their Yahoo mail accounts to mail themselves healthcare notes, or questions to ask the doctor. There is likely no major information system available online that is not “used as a PHR” by some patient.

Should the FTC consider all of these products to be Personal Health Record systems? Of course not, because they are not widely marketed to users as specific solutions for that particular purpose. This notion is encapsulated in the word “offers” in the FTC PHR definition.

We have detailed, extensively, how Facebook uses AI and machine learning methods to auto-suggest clinical Groups to users who search for clinical terms. We have detailed how Facebook likely uses data gathered from other sites in its algorithms to ensure that patients are matched into patient communities. More than any press release or blog post, this amounts to “offering” a PHR. Having offered a PHR, Facebook then allows the targeting of ads based on “interests in specific clinical topics”, ensuring that its PHR offering is profitable. This dynamic makes Facebook distinct from cloud-based offerings from other companies, who do not engage in the promotion of their products for clinical uses, or have specific mechanisms to profit from those clinical uses.

As a result, we argue that Facebook Groups is a PHR product, because:

- Facebook is aware that its Groups product is used as a Personal Health Record (PHR).
- Facebook advertises that these Groups should be used as a PHR.
- Facebook uses AI to detect clinical conditions in specific users.
- Facebook guides those users into clinical Groups that are acting as PHRs.
- Facebook allows advertisers to target users based on their interests in clinical topics.

If it looks like a duck, swims like a duck, quacks like a duck, it is a duck.

If Facebooks Groups product is a PHR under the FTC rule, then all or most of the data leaks that we document in the section above titled *“Facebook allowed substantial patient health information to leak”* count as breaches under the FTC Breach Notification Rule. We notified Facebook regarding its obligations, yet Facebook has not officially notified the affected individuals, months after the relevant deadlines have passed.

So far, Facebook has not even publicly acknowledged on its website that it changed the privacy settings of its Groups product. This stands in stark contrast to the similar changes it made to its API system, which is placed prominently in several places. In response to an article that was written after we contacted journalists at CNET, Facebook stated: "While we recently made a change to closed Groups, there was not a privacy loophole" So Facebook’s position has not merely been to not honor their notification obligations, but to specifically deny that there was any data breach at all.

Bear in mind that Facebook could have easily honored its obligations under the breach notification rule in a manner that would have been both effective and inexpensive. Because they have the capacity to both "message" and email users it has two mechanisms to directly contact all impacted users. Facebook was also constantly discussing privacy failures with reporters. It would not have been difficult to honor the obligations of the notification policy.

Being direct about this problem, and taking responsibility for this issue as a breach would have been relatively easy for Facebook, and yet they have done nothing.

All of the above violated 2012 FTC consent order.

These problems, taken together, clearly stand as meriting independent consideration as a new complaint. However, it seems fairly clear to us that many of these issues are also explicit violations of the 2012 FTC Facebook Consent Order.

Fine calculations

The maximum penalty for a "violation" of a failure to notify under the FTC PHR breach notification rule is $41,484.

The only reasonable way to count Facebook's violations is to count the number of distinct breaches that have occured, since the time when Facebook that knew that breaches were occuring. And count its continued silence and denial of the problem as counting as a distinct failure to notify for each distinct breach.

Calculating the number of distinct breaches should be the number of times a given user A was able to download or view the real names of Facebook users who were not already the "friends" of user A, who were the members of a Public, Closed or Secret group whose stated purpose was to provide support for a clinical conditions(i.e. the group was an instance of a PHR product).

We believe the appropriate time to start counting these breaches is the first time that Mark Zuckerberg explicitly endorsed a Group for the purposes of facilitating patient collaborations. The earliest date that this occurred that we have found was the 500 Million video on 7-21-2010.

However, we expect this data breach occurs several thousand times a day. We explicitly informed Facebook about the SicGRL (and other) breaches on May 29th 2018. That means that Facebook has failed to notify the users impacted by this breach for 163 days at the time of the submission of this compliant. Assuming Facebook honored its breach notification duty tomorrow, and assuming that 10000 such breaches of healthcare data (from not-Public Facebook Groups) occur each day, the fine would be:

10000 x $41,484 x 193 = (approx) $80 Billion

We believe that May 29th 2018 should not be the date from which Facebook should be fined per breach if it is shown that any employee ever explicitly warned Facebook leadership that the Group product was a PHR under FTC rules and that the privacy settings were causing ongoing breaches. In that case, the fine should extend to cover days since that notice was made.

Conclusion

Facebook actively solicited participation of patients in health Groups but then failed to protect their privacy, which was (1) unfair and deceptive; (2) violated the FTC PHR breach reporting rule; and (3) is also a violation of the 2012 consent order.

While the circumstances of the breach might have been deceptive, unfair and misleading, creating a problem for Facebook with the FTC, honoring obligations under the FTC breach notification rule would have been trivially easy for Facebook. Not honoring its obligation under the breach notification rule, given the fact that millions of patients might have experienced thousands of data breaches each, given the scale of Facebook's operation, could create an FTC fine obligation that could bankrupt Facebook hundreds of times over.

So…. Why risk it? Why would Facebook ignore a clear warning, delivered through multiple channels from the patient community that it had a problem with the FTC breach notification rule, when complying with the rule, and even correcting the ongoing breach, could have cost almost nothing?

More telling is the question that arises immediately after that: What, beyond a privacy analysis from a patient Group Administrator and qualified security researcher, would have gotten their attention on this, **or any similar**, issue? What else are they missing? What else are they ignoring?

Facebook seems to be deliberately ignoring the real privacy implications of its products. They noted in their response that Facebook places limitations on the transition between Secret->Closed->Public Group types. From their response to us:

We also have limitations in place to prevent Secret Groups, for example, from changing themselves to more open privacy settings after they exceed a certain size. This behavior is intended to prevent the ***negative experience*** *of having content you posted / a group you joined under one set of expectations being exposed more broadly.*

The emphasis is ours. We did not complain to Facebook regarding this issue. It seems that they know of **other** violations of users' privacy consent in their Groups products, or of the potential for abuse given the inadequate controls. They simply mentioned the new problem as "well this is really only one of the cases where our Groups product ignores the privacy decisions of our users", mentioning a problem that we did not even bring up to Facebook. Tellingly, they merely regard this violation of user consent and complete disregard for previous privacy decisions to be nothing more than a "negative experience."

It is obvious that Facebook cannot tell the difference between minor and major privacy problems. This would be like a restaurant not being able to tell the difference between: "Hey I do not like the hamburger you made me, it has mustard" and: "The hamburger you made me put me in the hospital with food poisoning." Facebook does not seem to differentiate between a user not enjoying a given action and that user being harmed as a result of an action. Their mental modeling of privacy issues does not seem to differentiate between: "These users are upset" and: "We allowed one user to change the privacy choices made by another user, and that got someone killed because they were recruited for fraudulent healthcare treatment, or targeted by a hate group."

Facebook is beset on all sides by privacy criticisms: Zuckerberg has been called before Congress. Facebook shareholders are revolting over privacy concerns, and wonder why Facebook is a public company yet remains immune from the will of the majority its shareholders. They have already received a "slap on the wrist from FTC regulators", which included very specific instructions on how **not** to approach these issues. Facebook has an exodus of users over privacy concerns. They know regulation is being considered to specifically target the platform. Facebook is constantly facing criticism in the press. They know they have a privacy problem that is bad enough that they are releasing TV ads. Facebook previously suffered problems similar to the ones that we highlighted, but with Apps and not Groups.

By all accounts, it is hard to imagine how Facebook could have reached the conclusion "this is a good time to ignore and then deny that we had a newly discovered privacy problem". And yet that is exactly how they responded to us.

What additional circumstances might Facebook need in order to be made receptive to a message with the content of "*Hey, there is a privacy problem which threatens the life and safety of many of your users. Here are the specific FTC regulations that apply to this situation that create clear obligations for your company. Here are dozens of approaches that you could take to fix the underlying problems. How else can we help*"?

The only reasonable explanation is that the current organizational culture, leadership, and business model of Facebook is irreparably incompatible with any concept of user consent, consumer privacy or existing FTC regulations. We, the Facebook users who have been hurt by Facebook's privacy policies, believe that Facebook cannot be reasoned with. Please consider this as you measure the FTC response to all of your investigations regarding Facebook.

Update Feb 16 2019: This document is now publicly available at
https://missingconsent.org/downloads/SicGRL_FTC_Compliant.pdf