

Facebook & Cambridge Analytica: What we know, what they knew & where that leaves us

Facebook's founder and CEO, Mark Zuckerberg, spent nearly five hours Tuesday answering questions from over 40 members of the US Senate Commerce and Judiciary Committees.

This appearance, and another one Wednesday with the US House Energy and Commerce Committee comes five months after Congress

first grilled the lawyers of Facebook, Google and Twitter on the platforms' exploitation by outside governments to influence the 2016 election.

Zuckerberg accepted the invitation to answer questions surrounding the sale and transfer of data – gathered without consent – of up to 87 million Facebook users, from a Facebook app developer to the data analysis firm Cambridge Analytica.

It's unclear whether Congress's interest in this matter is the result of either the size of the data exposed, the perpetrators involved or the results of the breach, i.e., how the ill-gotten data was used. Or perhaps the continuing onslaught of data breaches at so many other platforms and companies has made the legislature finally decide to step in on behalf of the American consumers and see what all those hotshot wunderkinds in tech are actually up to when they aren't otherwise "moving fast and breaking things."

Whatever the reason, the Eye of Sauron has now been fixed upon Facebook, Google and other platforms that traffic in user data. We can expect that they will now face the kind of scrutiny that has previously been reserved for large global companies such as Microsoft, AT&T and others. Though a more apt comparison may be the scrutiny and subsequent fines and regulation faced by the tobacco industry, which came under fire for the ways it sought to hide its products' known deleterious effects and the companies' efforts to increase their addictive properties and market them to an ever younger population, disregarding the interests of consumers. The Silicon Valley hoodie-and-Whole-Foods "disruptors" have now officially joined the big leagues and must come to grips with the great responsibility that comes along with their great power.

How Facebook responds to this crisis, and, more importantly, how users respond, could have a serious impact on the viability of Facebook as a dominant marketing channel.

Restrictions around data policy, data access, targeting capabilities and more will have significant downstream implications for marketers maximizing those very powerful tools that Facebook currently provides.

“Privacy is no longer a social norm.” – Mark Zuckerberg, 2010

Privacy last

Since leaving the Harvard dorm room Zuckerberg repeatedly referred to during the Congressional testimony (as if to say, “Aw shucks, we’re just a bunch of kids trying to make our way in this crazy, scary world of business”) and expanding beyond university campuses in 2006, Facebook has struggled with securing – and caring about – its users’ privacy. Mark Zuckerberg famously said in 2010 that privacy was “no longer a social norm.”

A small sample of early big stumbles

Playing hide-and-go-seek with privacy settings

Much of Zuckerberg’s testimony and responses this week centered around how the platform is (now) doing everything possible to make privacy and securing one’s data easy and understandable to users. There was no acknowledgement (and sadly, no significant pressure by any of the legislators on this issue) that Facebook has historically made it incredibly difficult for users to understand how, why and where they can limit sharing of and access to their own data on the platform. Over the years, there have been multiple updates to not just features and options, but changes to the locations for these settings and often, a reversal of previous user selections for controlling privacy.

In response to the crisis Facebook faces (It failed to fully act on Cambridge Analytica's purchase of Facebook data from Cambridge University researcher Dr. Kogan, which Facebook learned about over two years ago), the company has been racing to fix, clarify and improve users' abilities to control their own data and privacy settings and understand how their data may be used. In the past two weeks alone, the platform has announced:

Maybe it costs a life by exposing someone to bullies. Maybe someone dies in a terrorist attack coordinated on our tools. And still we connect people. – Facebook VP Andrew Bosworth

Growth at any cost

Facebook has never been particularly apologetic about anything it does. The company has been laser-focused on a single metric: growth. Growth of users globally across all of its products. Facebook has been incredibly successful in this mission – and the company's profits have followed its growth arc. Facebook couches this relentless pursuit of growth under the much more innocuous-sounding goal of "connecting people." Connecting people, making it easier for everyone to have unfettered access to information, social connection and so on is a truly worthy goal. I believe the people at Facebook have good intentions for reaching those goals. But I also believe they can be cavalier – and perhaps callous – in managing the path to that growth.

This was never more clear than in the statement that was made by Andrew Bosworth in a memo to Facebook employees in 2016: "So we connect more people. That can be bad if they make it negative. Maybe it costs a life by exposing someone to bullies. Maybe someone dies in a terrorist attack coordinated on our tools. And still we connect people." When questioned by Senator Lindsey Graham about this comment, Zuckerberg replied "Well, Senator, we try to run our company in a way where people can express different opinions internally," and noted

that he disagreed with the comment.

Disagreement, differing opinions, healthy debate – these things are all good and necessary within organizations. But the tone is set at the top. A long-time vice president making such a statement sets a tone, models a principle and impacts the organization as a whole. Continued growth, at the expense of user data security and user data privacy, is precisely what enabled data to get from Facebook to Cambridge Analytica, via the poorly vetted and monitored app ecosystem.

It would be possible for us to exist without a developer platform. – Mark Zuckerberg

App developers were key to Facebook's growth – and its security problems

Attracting developers to the platform has been instrumental in Facebook's growth. Apps not only attract users but increase engagement on the platform. And this is not unique to Facebook of course. It's been key to Google, Apple and Microsoft product successes as well. But each of the platforms handles their app and developer initiatives very differently.

The crisis Facebook (and up to 87 million Americans) face now is the direct result of a Facebook-sanctioned app improperly accessing user data without consent, and then selling that data to Cambridge Analytica. A primary question asked by at least half of the legislators yesterday and today has been, "When did you know about the sale of the data?" And while germane to the issue at hand, it ignores the bigger question that no senator pushed Zuckerberg on, which is, "Why didn't you vet the apps before?" Congressman Lujan from New Mexico finally addressed this question today, asking Zuckerberg specifically, if "Facebook knew about data scraping in 2013 and [data selling] in 2015... why did it take so long?"

Earlier today, in response to a different question, Zuckerberg said something to the effect of, “We thought developers telling us they wouldn’t misuse the data was enough.” This is either incredibly naive or an incredibly well-crafted position to take because it sounds better than “We didn’t want to limit-thus-dissuade developers from creating apps.” Or perhaps the company just didn’t want to dedicate engineering resources away from product development toward ecosystem oversight. It’s hard to know why the problem was ignored for so long because Facebook has not been incredibly transparent, despite being called to appear before Congress and the scope of this problem becoming public knowledge over the past several months.

Though noted by Zuckerberg that the first changes made to the third-party app TOS were announced in 2014 and enforced in 2015, it was not until last week that truly restrictive policies were clarified and put in place.

Congressman Loeb sack today asked if Facebook could exist without sharing people’s data with third parties. He replied, rather disingenuously in my opinion, “It would be possible for us to exist without a developer platform.” While that may be true now that the company has achieved the growth and maturity it has, would the platform be the behemoth it is if it had never had the developer platform in the first place?

Software isn’t eating the world – data is.

At the crux of issue being addressed is not just whether data has been improperly accessed, but what has been done with that data. And what impact does this current situation mean, not just for Facebook and marketers on the platform, but for other platforms, data providers and data brokers? This is certainly not the first massive exposure of data under a corporation’s control. This live, interactive visualization demonstrates just how frequently data gets improperly obtained and

information on people is exposed.

What has been surfaced with the Cambridge Analytica situation is how user data is used in a variety of ways – many unknown to the users themselves – and particularly in ways meant to influence thought and behavior. This data exposure has laid bare for the average citizen the volume of behavioral data being gathered and utilized for marketing purposes and the many usage scenarios applied – not just political – though that's at the heart of how Cambridge Analytica used the data.

Europe has been out in front of all issues related to privacy, user data, and sanctions for data mishandling. The forthcoming General Data Protection Regulation (GDPR) represents the strictest application of data management and user consent. And reiterated in testimony yesterday and today by Zuckerberg, Facebook is committed to applying GDPR to all users of their platform worldwide, though how it will be compliant across their products is unclear. Zuckerberg told the House today that there will be a tool at the top of the News Feed to walk users through the various settings and request consent. However, when asked by Congressman Green about the data portability portion of GDPR and how Facebook would implement compliance, particularly with respect to Custom Audiences data, Zuckerberg replied, "I'm not sure how we're going to implement that yet." This declaration of global support for GDPR is not insignificant and throws down the gauntlet to the other major platforms to follow suit. The impact across marketing campaign execution and customer data management, and the platforms and ecosystems that enable personalized marketing at scale cannot be understated.

Though focused first and primarily at political ads, the changes announced by Facebook over the past two weeks also impact ad targeting in other segments, availability of third-party data inside the platform and other limitations:

As many questions were left unanswered as were answered by

Zuckerberg, however. He managed to avoid answers to pointed questions about how much control users have over and visibility into the data that Facebook has on them. There were many questions by both the Senate and House members that demonstrated great confusion and understanding of how things actually work at Facebook, and disambiguation on the part of Facebook did not seem to be on the agenda. Many people in tech and tech news took away from those questions, “See? The government doesn’t get it. They don’t even know how Facebook works!” What I took away from it is that if the people in those chambers, with their vast resources and staff (usually younger than their own demo) can’t figure it out, can the majority of America really be expected to? And is it reasonable to expect that given the confusion around how data gets into Facebook – as well as out – your average user can be expected to adequately manage their security and privacy settings to prevent data sharing they don’t consent to?

Platforms and marketers are confronted with the looming GDPR compliance and similar other initiatives because as an industry, we’ve not been asking the right questions. Facebook’s coming changes are a nice start, but this is just the tip of the iceberg, and everyone needs to take a good, fresh look at how customer data is being gathered, used and protected to weather this storm.

[This article first appeared at Marketing Land.]

About The Author

Michelle Robbins, SVP Content & Marketing Technology, oversees editorial direction as Editor in Chief for Third Door Media’s

digital publications, Search Engine Land, Marketing Land and MarTech Today, directing a full-time staff of reporters and editors managing contributed content. She is responsible for developing the content strategy across all properties and aligning those initiatives with the programming and audience goals for Third Door Media's two leading marketing conference series, Search Marketing Expo and The MarTech Conference. In addition, Michelle oversees information technology operations, directing the marketing technology department. An experienced domestic and international keynote and featured speaker, she enjoys connecting with the community at SMX, MarTech and other industry events. Connect online with Michelle on Twitter @MichelleRobbins, and LinkedIn.

<http://feeds.searchengineland.com/~r/searchengineland/~3/njmY3qVnsvo/facebook-cambridge-analytica-what-we-know-what-they-knew-where-that-leaves-us-296107>