ISTOCK/GINTAS77

FACEBOOK

How to Manage Data Responsibly?

CAMBRIDGE ANALYTICA, FAKE NEWS, UNAUTHORIZED DATA SHARING: the crises are piling up for Facebook. Is it time for the social media giant to rethink its responsibilities for managing user data?

In January 2018, Facebook CEO Mark Zuckerberg announced a major change to the social media platform he founded. His stated purpose? To help users "have more meaningful social interactions."

"The first changes you'll see will be in News Feed," he wrote, "where you can expect to see more from your friends, family and groups (and) less public content like posts from businesses, brands and media."

The explosion of public content can be traced back to an algorithm change in 2009, which continued to be refined over the years, giving more weight to content that was "popular" in terms of having the most interactions and "engagement." The more popular the content, the higher it appeared in a user's News Feed. Many felt this was a move aimed at enticing advertisers.

Noting that "we built Facebook to help people stay connected and bring us closer together with the people that matter to us," Zuckerberg now said he was "changing the goal I give our product teams" to help "put friends and family at the core of the experience" because "research shows that strengthening our relationships improves our well-being and happiness."

Despite these heartfelt words, others had a less lofty interpretation. Many saw it as damage control in the face of mounting criticism. The rise of fake news, which spread like wildfire via the social media network, was increasingly suspected of influencing the 2016 U.S. presidential election. Though Zuckerberg had initially dismissed the idea as "crazy," by the time of his announcement he had admitted that he should have taken such claims seriously. By 2018, Facebook was making headlines for all the wrong reasons, coming under fire from users and regulators alike for its seemingly cavalier attitude toward data privacy concerns and its (mis)handling of controversial content.

In the Hot Seat

Data privacy concerns have been present since Facebook's inception in 2004. Its acquisitions of multiple tech companies over the years – notably Instagram in 2012 and WhatsApp in 2014 – have only fueled suspicion that user data was being cross-shared. Although Facebook insisted this wasn't possible, the European Commission fined Facebook $122 million for "providing incorrect and misleading information" about "the technical possibility of automatically matching Facebook and WhatsApp users' identities."

Users' lack of control over their personal information has always worried privacy watchdogs. Both Dutch and French regulators have levied separate fines on Facebook for failing to protect user data and for not adequately notifying users or obtaining their explicit consent for how their personal data will be used.

The straw that broke the camel's back was the news that the British consulting firm, Cambridge Analytica, had improperly harvested the personal data of up to 87 million Facebook users for political purposes. Exploiting a loophole that existed prior to 2014, a third-party app developer had gathered the data of not only Facebook users who had participated in its quiz, but also those users' contacts. The app developer then gave that data to Cambridge Analytica, which used it to build psychographic profiles of voters.

When Facebook got wind of this in 2015, it suspended the developer and Cambridge Analytica from its platform and took their word for it that they had destroyed the data. Since Facebook considered the case closed, it didn't bother notifying users or regulators about the incident.

And then the story broke in March 2018. After a long silence, Zuckerberg finally made a public statement, apologizing for "a breach of trust between Facebook and the people who share their data with us" and promising to "make sure this doesn't happen again."

Facebook subsequently updated its third-party data-sharing policies and announced it would audit all the apps that had accessed data prior to 2014. Though welcome steps, there was also a feeling it was too little, too late – and only after getting caught.

Were Facebook's priorities mistaken? Indeed, the company was moving into ever deeper data analysis and artificial intelligence, with the intention of creating algorithms that could better predict what users wanted to see or experience, all with the goal of personalizing its service. But were duties being neglected in this process?

Certainly, with the world's largest database of human activity in its possession, Facebook has incredible micro-segmentation abilities. But what are its responsibilities regarding the control and use of that data? What changes should Facebook make to safeguard privacy and answer the critics? Is it time to regulate the social media network? □

The case study **"Facebook's Data Debacle in 2018: How to Move on?"** by IESE professors Sandra Sieber and Robert W. Gregory is available from IESE Publishing at www.iesep.com.

The Facebook crisis has served to strengthen the regulator's hand.

Reinforcement for Regulation

by Fernando Pinillo Bun
General Manager, Roca Junyent

DURING A RECENT PRESENTATION AT OUR LAW FIRM, I was amused to hear the former head of Mobile World Capital Barcelona, Aleix Valls, describe Facebook as being in "the love business," since it's about posting likes and heart emojis to show how much we like something. That romanticized definition is certainly one way the world's largest social media network has tried to sell itself to us.

But it's also about something else. Facebook is a platform whose business model is fundamentally about leveraging user data; "the product" is the users themselves. In other words, Facebook makes money by selling advertising informed by and tailored to our interests, our passions, our activities and our groups. Of course, Facebook is not the only social media business to do this. As experts like Alberto Delgado, author of *Digitalízate*, have long attested, this business model comes straight from the digitalization playbook.

Knowing that, the most surprising aspect of the Facebook scandal is not the fact that the company was harvesting our data but rather that a company so good at doing it – seizing the opportunities and managing such extraordinary growth – could be so inept at managing the crisis after it became known that third parties had misused that data. I say "inept" because, even though any company would have a hard time owning up to a breach like this, Facebook didn't have to wait almost three years to finally acknowledge it publicly. This delay gave Facebook a serious perception problem in the eyes of its users that its response was too late, too reactive and too mild.

This hasn't just damaged the company's image, it's now going to have a major impact on data protection policies in general. Although new regulation on data protection was already in the works before this story broke, the Facebook crisis has served to strengthen the regulator's hand. There is now a far greater climate of acceptance of regulation than before, even though many of the aspects that are being seen as novel could have been dealt with under existing laws. The new General Data Protection Regulation (GDPR) that entered into force in Europe in May 2018 is much stricter than anything on the books in countries like China or the United States, where some legislators are now calling for EU-style regulation in light of the Facebook incident.

Perhaps another way to frame the debate is that users should be much more aware of what is being done with their personal information. We know our data is being used to build online profiles of us for increasingly sophisticated and sometimes subliminal advertising campaigns – yet only now is any concern being expressed, and online advertising is probably going to change shape as a result. We largely tend to ignore how our data is being handled when navigating the internet, simply out of sheer laziness or impatience to find what we're looking for.

Complacent attitudes and actions – not only on the part of Facebook but of us as users – make for an explosive cocktail that, if we're not careful, could end up limiting our freedoms more than any new regulation succeeds in protecting them.

Facebook needs to put users back in control of their personal information.

Restore the Right Balance

by Martin Breidsprecher
COO, Azteca America

DATA PRIVACY CONCERNS HAVE BEEN PRESENT for a long time – and in digital terms, 10 years is a really long time. As social media have become big influences in all our lives, governments and privacy watchdogs are paying greater attention to these concerns and taking them much more seriously. The Cambridge Analytica scandal, along with alleged Russian interference in the 2016 U.S. presidential election and signs of meddling in the upcoming U.S. congressional midterm elections, all have very negative implications for Facebook.

For social media companies, data-sharing is vital. Being able to detect patterns, influence behaviors and make predictions are key to serving users well and ensuring they continue being users. As such, how and with whom personal data is shared become central concerns in today's regulatory environment.

The fact that Mark Zuckerberg's response to the scandal was to announce that he was changing company goals to prioritize users' well-being implies that this was not the case before. The reality is that Facebook is a publicly traded company under constant pressure to increase its user base and report better numbers to please investors. Many public companies will recognize this inherent tension between users and investors; the key is not to satisfy one at the expense of the other. Yet that was what was happening, according to what a former Facebook manager told *The New York Times*: "The people whose job is to protect the user always are fighting an uphill battle against the people whose job is to make money for the company."

If we accept this as true, then winning back users' trust and working harder to keep it should be Zuckerberg's No. 1 priority. In all likelihood, privacy regulations are going to get tougher. And it's almost a given that additional cases like Cambridge Analytica will come to light, so Facebook should be bracing itself for additional fines and another hit to its reputation.

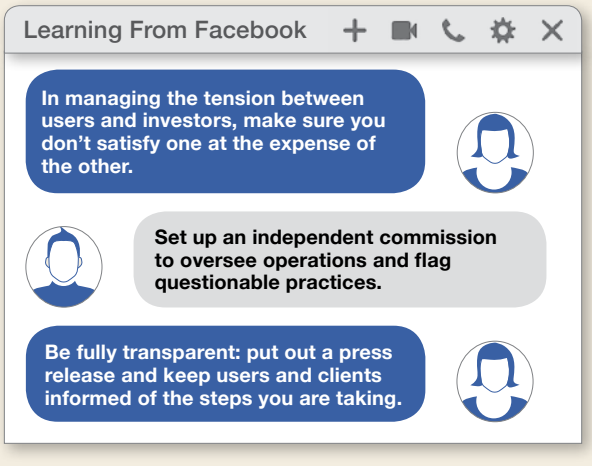
Users need to be in control of their personal information, and this is something that Facebook needs to assure them. It cannot continue with past practices of data-sharing and cross-sharing without the proper authorization of the end user. After all, it is his/her own data that Facebook is profiting from.

This is what I would have done differently. I would have proactively set up a separate, independent, autonomous organization – similar to a nonpartisan government commission – to act as a watchdog over my operations. This organization would interact directly with regulators around the world to address any questionable data-sharing practices, both those already identified as well as potentially damaging future ones.

Through this new entity, I would conduct a thorough investigation to find out what other personal data might have been shared with third parties. I would even put out a press release indicating what I am doing. Users and clients need to understand that I am treating this matter as a top priority and taking certain steps to make things right, even at the risk of bringing new cases to light.

Moreover, I would improve the data-sharing permission credentials, so users know exactly what they are allowing Facebook to do. This would have to go hand in hand with an intense marketing campaign.

There's no avoiding the fact that Facebook is going to take a short-term hit – sometimes this is necessary for the sake of some future gain. But taking actions like those suggested could help to position Facebook in the long run at the forefront of data-sharing integrity.



When users realize their information can be used against them, trust in the platform disintegrates.

A Blockbuster Scandal

by Ivan Olivé
Director of Sales & Marketing, Edebé Group

A DATA BREACH. The personal information of users being compromised and shared with third parties. No matter how commonplace this has become in our modern world, it never ceases to amaze me that when it does occur, yet again, it can still have the capacity to make headlines and stir public outrage. The new and different circumstances of the Facebook/Cambridge Analytica scandal is the latest case in point.

What made the story different this time around was that the Facebook user data was apparently used for political ends – ostensibly to influence the outcome of the 2016 U.S. presidential election to put an unlikely candidate, Donald Trump, in the White House. It's a story worthy of a Hollywood blockbuster, with conspiratorial undertones of *The Manchurian Candidate*.

As the outrage has grown, it has become increasingly apparent that Facebook made two grave errors. First, its failure to protect user data is not just a shocking oversight but could be tantamount to gross negligence or willful misconduct. A second, more egregious error was its failure to take swift action to stop third parties from corrupting its platform, not just as a precautionary measure but undeniably when it was brought to their attention that it had indeed happened.

We all know (or should know) that Facebook's business model is built on taking users' personal information and online activity, and using that as a means to sell highly segmented advertising. As soon as users realize their information can be used against them, they lose trust in the platform. They may even decide to quit Facebook and take their precious data with them.

No wonder this crisis seems bigger than others, because Facebook's entire business rests upon it. While it remains to be seen how much this will end up costing Facebook, its stock value has been impacted enough for Mark Zuckerberg to take action that he hadn't been prepared to take before, announcing a series of new measures to reinforce user privacy.

If nothing else, this crisis has several silver linings. First, no one can claim ignorance anymore about the massive amount of sensitive data that is being generated daily in the digital world and its nefarious consequences. Second, it may force greater transparency on how our data is used and what we will or won't allow. Finally, it highlights the need for greater regulation and control over internet companies. Even Zuckerberg has grudgingly acknowledged that more regulation of social media is "inevitable."

Easy access and modification of our personal data, free portability of data between platforms, protection of said data, and the right to privacy are increasingly important concepts in a digital environment whose lightning-fast progress always outpaces regulation.

As we have heard countless times, data has become the oil of the 21st century. New business models, new uses and numerous innovations revolving around data will continue to emerge. But what we've also learned in light of this scandal is that everyone who lackadaisically gave permissions to countless applications, websites and social media networks will be much more aware of the possible implications of doing so from now on.