Cambridge Analytica Scandal:
Don’t Blame Facebook.
Blame Bad Ethics.

Executive Summary

On March 17, *The New York Times* reported that consulting firm Cambridge Analytica misused personal data on more than 50 million Facebook users in order to manipulate the outcome of the 2016 presidential election. Though politics are the central theme, the incident has also raised questions about the implications of marketing influence in a modern world — marketing driven by data.

We understand that marketers may be facing questions and second-guessing strategies involving data science, predictive analytics, targeting, data privacy and Facebook itself. This POV breaks down the reported scandal, clarifies what pertains to pharma marketers, and lays out recommendations in light of the news.

Short on time? Jump to our seven key takeaways, which include:

1. **Go small.** Capture only the minimum data needed.
2. **Be transparent** about how you use data.
3. **Ask the right questions** of your agencies and vendors regarding data collection, use and ownership.
4. **Understand regulations,** such as the EU’s GDPR, which goes into effect May 25.
5. **Seek pharma-friendly partners** that understand the regulations and risks.
6. **Protect your own privacy.** To protect your own privacy on Facebook, see this guide from *Wired*.
7. **Don’t despair.** Don’t let current events sour your view of the powerful possibilities of marketing in a data-driven world.

Background

On March 17, *The New York Times* reported breaking news involving Facebook, the Trump campaign, and a political consulting firm named Cambridge Analytica (CA). It was reported that CA had gained access to the data of more than 50 million Facebook users and misused that data for political influence during the 2016 presidential election. Here’s a breakdown of what happened:

1. In return for $1 – $2, roughly 270,000 people downloaded a Facebook app called “thisisyourdigitallife.”
2. With users’ consent, the app pulled information from their and their friends’ Facebook profiles.
3. The researchers who created the app then passed the data to CA without users’ permission — a violation of Facebook policy.
4. The data was then allegedly used by CA to build psychographic profiles of users and their friends, to help the Trump campaign identify voters for targeting, to provide advice on where to focus campaign efforts, and even what to say in speeches.

The scandal has raised concern about the privacy and security of Facebook data, not to mention legal questions around CA’s business practices. But the implications could be further reaching, calling into question ethical concerns around the exploitation of user data to manipulate behavior.

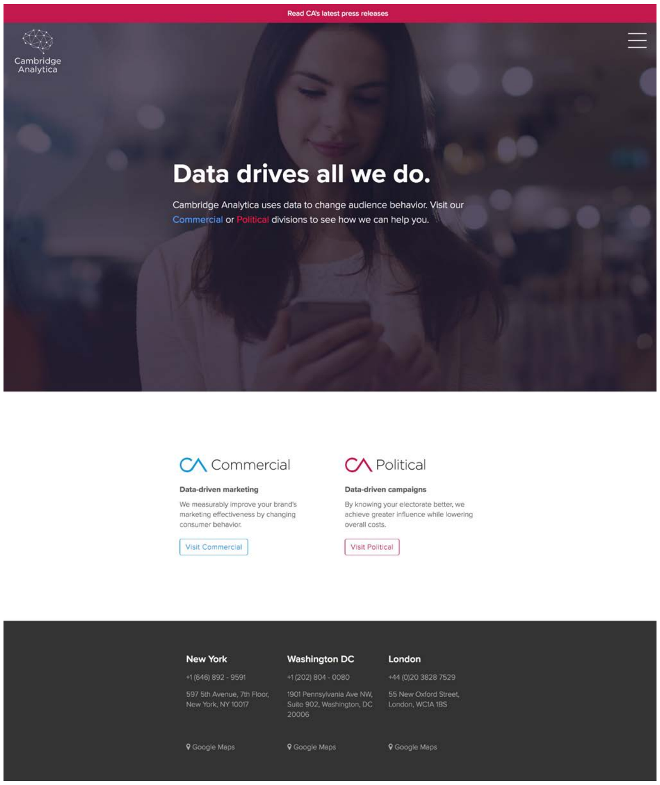
Next, we’ll break down these current events from two different marketing perspectives — data science, and Facebook.

How Did Data Science Play a Part?

The use of data for predictive capabilities in marketing has been around for years. Retail giant Target’s marketing algorithms famously exposed a teen girl’s pregnancy, much to her father’s dismay. But CA’s use of data was something different altogether:

- **The data:** Misappropriated data included names, gender, locations, and Facebook “likes.” The app itself was veiled as a personality quiz and included questions on respondents' political leanings.

- **The intent:** Reports detail CA's intent to use the data to build algorithms to predict personality traits of voters, and then influence them. In an interview on NBC's "Today," a former CA employee said CA used the data to "create a web of disinformation online" and exploit "the mental vulnerabilities of people" with targeted political messages.
- **The denial:** CA has repeatedly denied that it used any of the data to influence the Trump campaign outcome.



Read CA's latest press releases

Cambridge Analytica

Data drives all we do.

Cambridge Analytica uses data to change audience behavior. Visit our Commercial or Political divisions to see how we can help you.

CA Commercial

Data-driven marketing

We measurably improve your brand's marketing effectiveness by changing consumer behavior.

Visit Commercial

CA Political

Data-driven campaigns

By knowing your electorate better, we achieve greater influence while lowering overall costs.

Visit Political

New York
+1 (646) 892 - 9591
597 5th Avenue, 7th Floor,
New York, NY 10017
Google Maps

Washington DC
+1 (202) 804 - 0080
1901 Pennsylvania Ave NW,
Suite 902, Washington, DC
20006
Google Maps

London
+44 (0)20 3828 7529
55 New Oxford Street,
London, WC1A 1BS
Google Maps

Personal data can be used to predict moods, emotions, personalities and a long list of other traits and intentions. The rise of the digital channel and the rapidly growing availability of legally acquired data have even further expanded these possibilities. In fact, healthcare companies and partners like Intouch have been practicing ethical predictive modeling for years — with an aim to target the right customers and serve relevant information to them.

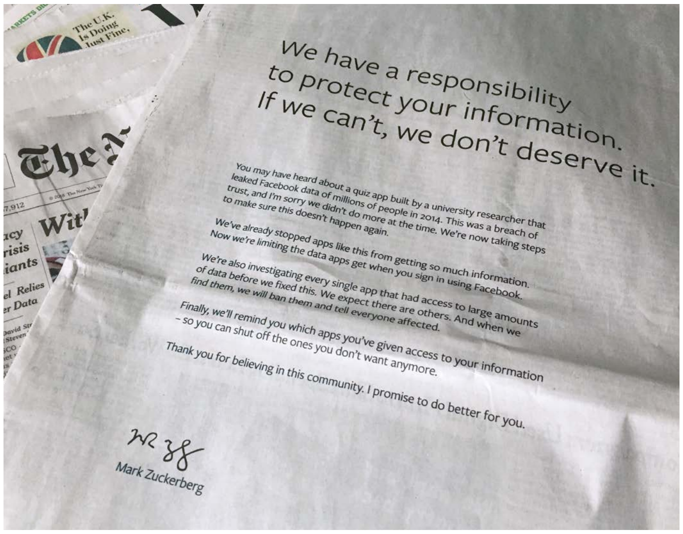
The difference? Ethics.

Is Facebook a Safe Place to Be?

To be clear, this incident was not a Facebook data hack, leak, or breach. While the data was mishandled by the researcher, it was originally accessed legally and within Facebook's rules at the time.

If your brand or company currently hosts a Facebook page, there's nothing you need to do differently; none of that data was compromised.

It's worth noting, however, that users — including Tesla CEO Elon Musk — are deleting their Facebook accounts in the face of the trending #deletefacebook movement. The *Wall Street Journal* reports that some companies have suspended advertising. Facebook's value dropped by nearly $50 billion since the news broke. To mitigate damage, Facebook has been reaching out to companies, industry groups, and agencies to reassure them of data-privacy rigors, and Mark Zuckerberg issued an apology in a full-page ad placed in American and British newspapers. The following day, the Federal Trade Commission (FTC) confirmed it was investigating Facebook's data practices.



We have a responsibility to protect your information. If we can't, we don't deserve it.

You may have heard about a quiz app built by a university researcher that leaked Facebook data of millions of people in 2014. This was a breach of trust, and I'm sorry we didn't do more at the time. We're now taking steps to make sure this doesn't happen again.

We've already stopped apps like this from getting so much information. Now we're limiting the data apps get when you sign in using Facebook.

We're also investigating every single app that had access to large amounts of data before we fixed this. We expect there are others. And when we find them, we will ban them and tell everyone affected.

Finally, we'll remind you which apps you've given access to your information – so you can shut off the ones you don't want anymore.

Thank you for believing in this community. I promise to do better for you.

Mark Zuckerberg

If you're advertising to consumers on Facebook, it's understandable you may be concerned. While the incident represents a crisis of confidence, Facebook targeting and advertising remains safe for users and effective for advertisers.

Summary & Key Takeaways

Facebook is facing what may be its biggest crisis yet. Understandably, consumers are concerned about the misuse of personal data. And while this incident is borne from politics, a healthcare-related scandal could play out far worse from a privacy, trust and public relations perspective.

We work in a highly regulated industry. But some may be surprised to learn that regulations such as HIPAA haven't necessarily kept up with the evolving practice of data science.

Data regulations in the European Union (EU) are decidedly stricter than the U.S., and soon will become even more so as General Data Protection Regulation (GDPR) goes into effect. But GDPR, HIPAA and other health-data regulations won't stop unethical, unscrupulous people, or others who just aren't paying attention. This is why operating ethically is so important, and why asking the right questions up front is critical.

Seven Key Takeaways for Pharmaceutical Marketing

1. **Go small.** When capturing data yourself, capture the minimum needed. "... Avoid using a device that is capturing 20 different types of data if the research team's need is just for five," Pfizer's Craig Lipset recently told *MM&M*.
2. **Be transparent** about how you use the data you collect, regardless of the source. And once you have it, keep it secure.
3. **Ask the right questions** of agencies and vendors regarding data collection, use and ownership. Here's a starter list:
   - » What are the sources of the data?
   - » Is the data you are purchasing first-party data or third-party data?
   - » What are the terms of use and privacy policies of the data provider(s)?
   - » What are the opt-out policies and procedures?
   - » How recent and up-to-date is the data?
4. **Understand new regulations.** Be aware of new EU regulations going into effect May 25, and how they may affect your marketing plans. Businesses will need explicit consumer consent to use audience data, making third-party data more difficult to access.
5. **Seek pharma-friendly partners.** Ensure your direct data partners and agencies are experienced in healthcare and pharma. Not just for legal, regulatory and data-privacy expertise, but also to ensure they are savvy to the inherent risks in pharma communications.
6. **Protect your own privacy.** We're not deleting our Facebook profiles anytime soon. If you're interested in doing more to protect your or your family's Facebook privacy and security, see this handy guide from *Wired*. Or watch for Facebook's own new centralized page for controlling privacy and security to come soon.
7. **Don't despair.** Don't let current events sour your view of the powerful possibilities of data science, predictive analytics, targeting, or Facebook. In this case, technology wasn't the problem. Data science was not the evil. Facebook itself wasn't even the evil. People were.

Ultimately there are still more questions than answers when it comes to the ownership of data, the gray area of when exactly data becomes "health" data, and oversight to avoid future problems like the Facebook/Cambridge Analytica scandal. Some are calling for in-house tech ethicists to be installed before a larger crisis occurs. The Advertising Research Foundation said it plans to work with other trade groups to form new industry guidelines for consumer data collection, privacy and protection.

Time will tell if this incident will generate further regulation, if it triggers a downward spiral for Facebook as advertisers and users abandon the platform, or if instead, it just fades into history as a small note of caution.

Join the conversation: email us at getintouch@intouchsol.com, message us on social media, or contact your Intouch team.

Authors: Wendy Blackburn, Andrew Grojean, Sam Johnson, Aaron Uydess

Kansas City
7045 College Blvd.
Suite 300
Overland Park, KS 66211
p 913.317.9700

Chicago
205 N. Michigan Ave.
Suite 3200
Chicago, IL 60601
p 312.540.6900

New York
469 7th Ave.
10th Floor
New York, NY 10018
p 646.795.3600

London
2 Kingdom St.
London
W2 6BD
p +44.20.32392129

Mumbai
B-301, Flexcel Park, S.V. Rd.
Jogeshwari West
Mumbai, Maharashtra, 400102
p +91.22.26770010

Want to learn more?
Contact Wendy Blackburn
wendy.blackburn@intouchsol.com
intouchsol.com