Hacking Your Vote From Inside Your Head: How Cambridge Analytica Altered Reality Via Social Media To Induce Specific Voting Behavior

Anton Janik, Jr.
ajanik@mwlaw.com
(501) 688.8888

03/22/2018

We learned some important lessons this week about the dangers inherent to losing control of your customer or client data, either through hacking, internal theft, or poorly designed controls over what your business associates have access to or may share themselves. That case in point is Cambridge Analytica.

Last Friday evening, Facebook suspended the accounts of Strategic Communication Laboratories (SCL) and its affiliate Cambridge Analytica. (SCL created Cambridge Analytica. Cambridge Analytica was funded by Robert Mercer and had Steve Bannon on its board of directors.) Back in 2015, Cambridge Analytica began receiving Facebook user profile data from the myPersonality app, which was being used by Cambridge professor David Stillwell to understand and measure personality traits. Stillwell was able to track the scored personality traits across the app's user base, and to correlate app scores with Facebook likes. The Guardian reports this was groundbreaking in the way that it revealed correlations between personality traits and measurable behavior via likes; that is, by knowing the pattern of a user's likes, you could determine their personality traits.

The personality type correlation patterns that Stillwell discovered could be used in wholly different ways. That's where Christopher Wylie came in. While studying for his PhD, he found a paper discussing how personality traits could be a precursor to political behavior, i.e., determining likely voting behavior. One just needed to acquire a sufficient data set covering that voting pool, and a known set of likes to define those that vote in a particular way.

After graduation, Wylie was hired by SCL, who was in the process of gathering a large Facebook dataset. The reports are not yet clear on whether the data just came from the above research group, or from a Russian data miner Aleksandr Kogan, or from a combination of both, but in any event, Wylie revealed in a fascinating interview by The Guardian, that the effort resulted in the gathering of approximately 50-60 million Facebook accounts, including users' status updates, likes, and potentially, private messages. There have been some investigative reports stating that at least some data came from the app which had been granted special permissions to gather not just the personal data of consenting users, but also the same data for all of those users' Facebook friends—without ever seeking or being granted such access from the Facebook friends themselves.

What was most fascinating about the above interview, was that Wylie walked through how Cambridge Analytica manipulated data outside Facebook to induce behavior among those Facebook users. Wylie says that through a process of datamining, they learned what kinds of messaging each Facebook user would be

susceptible to, as well as the framing, topics, content, tone, and scariness level of the needed messaging, where the Facebook user would consume that messaging, and how many times Cambridge Analytica would need to "touch" the Facebook user with that messaging in order to change how the Facebook user thought about an issue. Then, Cambridge Analytica used its data scientists, psychologists, strategists, and creative team of designers, videographers, and photographers, to create content including blog postings and websites which was sent to a targeting team that injected it into internet. As Wylie says, "whatever we think this target will be receptive [to], we'll create content on the internet for them to find, and they will see that and click on it and go down the rabbit hole until they start to think something differently." As Wylie points out, this strategy was so successful because of the ability to mine the data so granularly that, "you are whispering into the ear of each and every voter; you may be whispering one thing to this voter and something different to that one" all of which induces the particular intended outcome.

This was the part that I found so fascinating: his discussion of the active creation of misinformation, false narrative, and other false sources to generate a push upon that particular Facebook user to move them to the favored decision point. Cambridge Analytica created a bubble of false reality to induce a predetermined outcome in actuality. This isn't an issue of leading a mouse with cheese. It's actually an issue of creating an individualized maze that leaves the mouse with the false belief that it has freedom of choice, while all the time the cheese and the path to it were chosen for it. I suppose the question remains as to whether the mice now know they were caged the whole time, or still are.

When asked why Cambridge Analytica did this work, Wylie stated, "if you want to fundamentally change society, you first have to break it. And it's only when you break it that you can remold the pieces into your vision of a new society. This was the weapon that Steve Bannon wanted to build to fight his culture war."

In the coming days, we may well learn that this data loss was just the tip of the iceberg, or of a fleet of icebergs, and that other businesses have acquired similarly wide swathes of data without user consent. It may turn out that the acquired data has not been properly secured since acquisition and has continued to disseminate across the web, or even the dark web.

The Cambridge Analytica lesson is important to your customers and clients because it facets just how damaging data losses can be. That is, data from one or more sources can be aggregated, segregated, and weaponized in ways that the data repositories could never have anticipated. And once lost, cannot easily be recaptured. So this brings us back to simple root precautions: pay attention to what data you have, how it is held, and who has access to it. Encrypt your data. Penetration test your repositories and their access tools. Keep on top of your access rights, to whom those are granted, the scope of the data they may retrieve, and what they must do with that data at the end of the project. Audit them for compliance. Finally, make sure to review your business associate agreements for contractual obligations governing the foregoing.