What the Zuckerberg Testimony Reveals About Modern Marketing and Data Privacy

Posted by Derek A. Lackey, Editor / June 11, 2018

Consider this: Your organizations data gets stolen by cybercriminals, resold, combined and aggregated with intent and behavioral data scraped from Facebook and sent into the hands of a data broker. MarTech vendors buy that data from the broker and sell it back to you as a marketing service, for you to better target and engage your customers and prospects. This is the data economy we live in, and its unintended consequences on data privacy are just starting to unfold.

Were beginning to understand how revealing our digital behavior can be: Stealing a credit card is one thing but being manipulated is something else entirely.

As with the rest of the world, marketing has gone digital. Data is the new currency, with many companies making more from the data they capture than from the actual goods or services they sell. This means risk from compromised, manipulated or stolen data for any organization handling that currency.

Its time for us to stop thinking about cybersecurity and risk as someone elses problem. As marketers, we are both consumers of big data and targets for cybercriminals who want access to our data for nefarious purposes. Everyone wants to learn how to better use machine learning and artificial intelligence to improve targeting and reach audiences. Too few want to think about the implications.

Security, data privacy and data governance need to be topics of discussion. Lets face it: The marketing industry is on the brink of disruption, caught in the crosshairs between modernization, malice and mandates.

TheFacebook/Cambridge Analyticacontroversy is a cautionary tale for anyone who thinks otherwise. Admit it, people knowing our online browsing behavior is creepy. Just yesterday, I was being pitched by a major MarTech vendor who was bragging about looking up browsing data for everyone in the room before the meeting.

Nowadays, behavior and intent data for every online user is being collated into personal digital dossiers that can be assembled from a combination of sources. Cybercriminals hack, collect and sell data anonymously and illegally in an industry with damages projected to reach$6 trillion by 2021. Data brokers get user info from sources they are vague to reveal, or legitimately, when we click the accept box for online services terms and conditions.

Facebook, Google and thousands of other MarTech companies are in the business of advertising and buying and selling data. We marketers are in the business of using the data to persuade people. The problem in the digital world is what users see is no longer in their control. Were seeing digital propaganda manipulate behavior and destabilize key institutions like democracy. Thats the fundamental shift changing the way we look at the power of big data.

That covers the consumption side, but why would your data be a target for cybercriminals? Stealing credit card data makes sense; itssold for around $10 a pop on the dark web. But why do people hack prospect, customer or behavioral data? Probably to sell it back into the data supply chain to data brokers. Its like thieving merchandise off a truck and reselling it cheaper on Craigslist.

New Pressures for Data Privacy & Governance

People love the idea of free online apps. They dont love that our private data is being used to target and influence us, which lets be honest is the core of what Marketing wakes up every morning to do. In the interest of driving accountability, governments and regulators are putting mandates in place to give users more control over their personal data.

TheEuropean Unions General Data Protection Regulation (GDPR)establishes a single set of rules to protect the personal data of EU citizens and violations can cost a company up to 4 percent of global revenue. The GDPR can be summed up this way: You must know where your data is, who has access to it and how its being protected.

The Digital Multiplier Effect and the Digital Marketing Risk Paradox

The Digital Multiplier Effect means what happens in the physical world is multiplied in the digital world. Take cybercrime as an example. Its easy to understand why online bank fraud or stealing credit card numbers is more appealing than physically robbing a bank. Crooks can anonymously steal more money from more people, with less risk of getting caught.

With MarTech there is a paradox. With modern tools and techniques, we can use more data to target more people, more precisely exposing them to more personalized messages than ever before. However, the paradox is our organizations are MORE at risk, not less.

First, its harder to control permissions and the right to be forgotten core tenets of data privacy. Second, if you ask even the most sophisticated CMO or digital marketer where their data is, who has access to it and how its being protected, youll get a long pause. A modern marketer is typically managing a virtual infrastructure that integrates an average of 84 individual cloud-based tools or applications. And it wasnt built end-to-end with cybersecurity or data risk in mind.

Lets say we went through all the security assessments for these vendors (which only 10 percent of companies say they do) and they all passed. There are still APIs built by various people, and the whole thing is managed by many different employees, agencies and third parties. No one is monitoring it end-to-end for cyber incidents or breaches, leaving us with an unmonitored, highly vulnerable, complex system,

which is the enemy of security.

Based on...

Read The Full Article