Pipeline
Technology for Service Providers.
www.pipelinepub.com Volume 14, Issue 2

Cambridge Analytica and AI - The Unignorable Lesson for CIOs

By: Praful Krishna

Cambridge Analytica, the political consulting firm that worked for the Trump campaign and harvested raw data from up to 87 million Facebook profiles, has folded. In the wake of Facebook's congressional hearings and the role Cambridge Analytica played in the Trump's election campaign, considerable concerns have surfaced.

Facebook has long been regarded as the trailblazer in social media. However, how much can users *really* trust platforms like Facebook with their data? In this case, a third-party developer exploited a loophole in the system to gather information on users—as well as users' friends—without them knowing. Facebook knew—and did nothing.

Zuckerberg faced one of his most stringent tests in the uncomfortable questions by senators on Capitol Hill. The job of CEOs and CIOs could become even harder if the U.S. decides to follow the lead of the European Union, which is set to embrace the EU General Data Protection Regulation (GDPR) that went into effect on May 25, 2018.

This episode comes at a time when CIOs across sectors, especially service providers, are thinking of adopting AI. There are profound lessons for everyone to study.

The rise of AI as the New Masters of Data

Ten years ago, social media was in its adoption curve where AI is today. Large companies are rapidly embracing the idea, and only opening to adoption now; a study by Adobe says only 15 percent of enterprises are actively using AI, while 31 percent are expected to add it in some form or another over the coming year. As most of its breakthrough abilities continue to unfurl in the fields of finance, healthcare, agriculture, manufacturing, technology, and countless other areas, an overlooked detail is that data fuels this technology.

In the coming decade, access to data to train AI and its wise usage will create winners and losers in the business world. As data becomes the new valuable commodity replacing oil, it's natural that the companies developing AI products will be eager to improve their AI engines to offer better products and services. Moreover, this can happen only when they get more and more data from their clients.

There are nascent algorithms like Calibrated Quantum Mesh, or applications like cognitive automation, which differentiate in that they need very little data to train. However, it is still meaningful. Additionally, even if they don't need data to train, they process enterprise data—or have access to it.

In other words, AI product companies are potentially getting data out of their client firewalls and exposing it to all kinds of risk. Enterprise data is, in most cases, customers' data metamorphosed. It took various high-profile data breaches for organizations to stop working under the assumption of "if," and build strategies around "when" a data breach will occur. Similar is the case for ethics when it comes to customer data. When customers register to avail any new service or product from a business, they put their faith in that business to protect their data. It's the responsibility of enterprises to protect that data at all costs.

A new study from Accenture shows that the scope of digital risk has expanded beyond cybersecurity and privacy into what is coined as digital ethics. Enterprises can't deny their responsibility for what they do with the customer data. Yes, it's about ethics now—how enterprises act on the data they collect and analyze has come under the scanner. The study says that in the future digital economy, enterprises and government agencies that achieve the proper balance of managing security risks and building digital trust effectively will thrive.

It's critical that enterprises integrate ethical data practices throughout their business processes with more robust ethical controls.

AI Product or AI Solution – The Nuance Matters

CIOs need to be careful. Let's say that, with appropriate diligence, they are able to find trustworthy product vendors that can minimize security breaches. Still, they would have given their most important competitive advantage—data—for the benefit of the product vendor and, by implication, their own competitors. The idea that started in an attempt to strengthen the company's competitive differentiation may end up achieving just the opposite.

Balancing data privacy and innovation is a tightrope walk. Amid all the debate about data privacy and controls, there is a renewed vigor to restore public faith in the technology. We need what can be called an AI 'responsible enough' to tackle this crisis. This Responsible AI is all about aligning an enterprise's AI pursuits with its core values and ethical principles so that it can benefit customers, employees, the business, and society. In the long term, this could create a ripple effect and build trust.

AI solutions are coming closer to being responsible than AI products. AI solution vendors design bespoke solutions for clients. In most cases, they deploy such bespoke solutions over a customer's private cloud or on-premise infrastructure. Responsible AI vendors ensure that not a single byte of data leaves the security of a client's firewalls.

There are other advantages. AI solutions are bespoke. They configure to an enterprise's need better than any AI product ever could. They are also trained specifically, making them more accurate. Still, these considerations dwarf what Cambridge Analytica taught all of us: entrusting data to third parties outside a firewall's protection is always dangerous.

In particular, there are a couple of AI solutions companies on the horizon that recognize the potential roadblocks inherent in this direction (both concerning data security risk, PR, and competitive differentiation). They understand the need to protect sensitive customer data at all costs, even if it means slowing things down on the AI front. Examples include giants like Microsoft, upstarts like Coseer and, to an extent, even IBM Watson.

A Virtuous Cycle of Virtue

Trust from enterprises and from their customers is going to be important for AI vendors as well—

solutions and products alike. It is not just about the compliance or ethical risks. This trust is going to be important for the accuracy of the solution as well.

AI systems don’t only learn from the initial training data; their learning continues as more and more users interact with them. AI systems that can win their users’ trust and provide better user experience will see more adoption. Their targeted users will prefer these systems over alternatives. This higher traffic would, in turn, train the AI system better so that it can provide even better user experience.

In other words, maintaining users’ trust using responsible privacy practices is beneficial not only to enterprise CIOs, but also to the business of AI solution providers.

The Journey Forward

The journey forward is indeed murky. However, tech revolutions have always happened nevertheless, changing the lives of an entire generation. In the long term, enterprises need to stay vigilant; consumers need to be ready to ask the hard questions and pay attention to what happens with—and to—their data.

As this wonderful technology evolves, responsible AI needs to partner with responsible CIOs—those who understand the appropriate importance of data security and the nuance between AI products and AI solutions. Government and leaders (in public and private sectors) have a role to play as well. They need to be made accountable for long-term as well as short-term thinking. The future is ours to take!