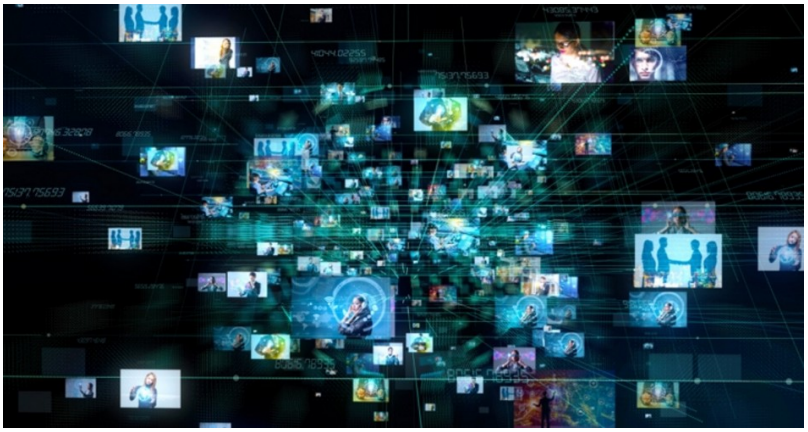
Written by **C. Mitchell Shaw** on December 9, 2018

# Big Names in Big Data Continue to Harvest Users' Data, Put Users at Risk



In the wake of the British Parliament's release of e-mails detailing Facebook selling access to users' data, more information is coming to light showing that this revelation may be only the tip of the iceberg. Big Data — including big tech companies, grocery store chains, retail chains, and others — harvest users' data and use it to create startlingly accurate dossiers of users. They use that data for their own targeted advertising and sell it off to others to use, as well.

Internal e-mails among Facebook staff showed that the company allowed external companies, such as AirBnB, Tinder, Netflix, Lyft, and others unhindered access to the data of those who use the social media platform — granted that those companies spent enough on advertising with Facebook. In the wake of the Cambridge Analytica scandal in March 2018, the e-mails shine a new light on Facebook's practice. The e-mails also show that Facebook CEO Mark Zuckerberg — who claimed to be surprised that developers could "abuse" the system that granted them such easy access to users' personal data — had been warned all along of the very real risk of that happening.

As the *Wall Street Journal* reported last Wednesday:

> The documents show Mr. Zuckerberg seeming to dismiss the risk of developers sharing Facebook data among themselves. That issue has been under scrutiny this year after the company disclosed in March that one developer had shared Facebook user records with Cambridge Analytica, a political analytics firm employed by the Trump campaign in 2016. Many lawmakers and other critics have said Facebook executives, including Mr. Zuckerberg, were naive about the risks in allowing open access to user records.
>
> In one October 2012 email to then-Facebook executive Sam Lessin, Mr. Zuckerberg said he was "generally skeptical that there is as much data leak strategic risk as you think," according to excerpts in Wednesday's release.

Another e-mail thread from 2012 shows Zuckerberg proposing a plan wherein developers would "pay 10 cents per user to tap information about their users' friends on Facebook," according to the report by the *Journal*. That plan would have paid huge dividends to the developers who would have chosen to pay 10 cents per user for access to the hundreds or thousands of "friends" of each of those users. It would also have paid huge dividends to Facebook.

But, Zuckerberg — realizing the profits to be made from data-mining the personal information of users — elected to put in place a plan that he liked even better. According to the *Journal*, "Mr. Zuckerberg ultimately said he would rather data access be free — so long as developers made it simple for their users to pass the data back to the platform." In the e-mail detailing that decision, Zuckerberg — showing that his ability to judge right from wrong is skewed — wrote that giving developers access to

data without charging them a fee "may be good for the world but it's not good for us unless people also share back to Facebook and that content increases the value of our network."

Ashkan Soltani, a former chief technologist for the Federal Trade Commission (FTC), who has criticized Facebook in the past, said the released e-mails "not only show evidence of wrongdoing with regards to user privacy, but they demonstrate substantial anticompetitive practices in the way they leveraged user data." The FTC has been investigating whether Facebook violated a consent decree from 2012 in which the company agreed to obtain user consent for collecting personal data and sharing it with others. Given that many of the e-mails recently released post-date that decree and show Facebook continuing to do exactly what it agreed not to do, the tech titan may soon find itself in very deep trouble.

But Facebook is far from alone.

Days after the Facebook e-mails were made public by the British Parliament, the *Daily Mail* is reporting on the "disturbing scale of the personal data harvested and traded by" multinational corporations. The report lists as examples of data harvested and used/sold by giant firms:

- Pregnant women's due dates being farmed out by Asda to mystery third-party companies for marketing;
- Children's voices recorded on the YouTube Kids app being used by Google to promote other apps;
- Passport photos given to PayPal for account verification may be shared with Microsoft for fraud prevention and the testing of new products;
- Health details, ethnic origin and political views of Facebook users being used by the social network for targeted advertising;
- Viewers of BT television being profiled for advertisers according to profiles of their television watching and telephone call records.

According to the *Daily Mail*, Marriot International "routinely stores the names and ages of its guests' children, room service orders, social media accounts and employer details and shares this across its operations in 150 countries." Some of those "150 countries" include oppressive nations, such as Venezuela, Gabon, and Libya which are far from friendly to the United States and its citizens.

Marriott is facing investigations by the UK Information Commissioner's Office as well as the FBI and five states in the U.S. Last week, Marriott reported that its database — including all of that sensitive data on its guests — had been breached by hackers. Those hackers managed to steal the data of at least 500 million of those guests.

Other companies that routinely collect and use/sell users' data include Google, PayPal, Amazon, and too many others to list in the space afforded to this article.

As reports of this type become more and more commonplace, one sentiment that often arises is typified by the questions, "What is the big deal?" "Why should I care that Facebook or Google or Amazon or any other company uses my data for marketing purposes?" "If I don't have anything to hide, why should I care?"

This writer actually began his writing career answering those questions and pointing out some tools and tactics that can be used to protect your privacy online. An indispensable part of answering "why it matters" is found in an understanding of how data-mining and data-analysis work together. As this writer explained in one of those early articles:

> Data mining is a big problem, as we saw from the documents leaked by Snowden. But there is more to it than most people realize. In 2012, a father of a teenage girl saw for himself how powerful this form of information gathering and analysis can be. Several years ago, Target department stores started offering Redcard. It's a credit or debit card that can be used to make purchases at Target stores and on their website. It offers a five-percent discount any time it is used. Target's reason for doing this is simple. It ties all of your purchases together into one profile for data-analysis purposes so that they can send you advertising based on not just what you buy, but what their data analysis tells them you are going to buy. How effective is it? The father of that teenager stormed into a store outside Minneapolis and demanded to know why his daughter was receiving advertisements for baby clothes, baby furniture, and diapers. After all, she is still in high school. The manager said he would look into it and call the father in a day or so. When he called two days later, the father said that he had talked with his daughter and learned that she was, indeed, pregnant. Target figured it out before her own father did.

This writer further explained the importance of data-mining and data-analysis in a subsequent article:

> Now, if Target was able to accurately predict a teenage pregnancy based only on subtle changes in purchasing habits at their stores, what could be known by compiling and analyzing *all* of the data on *all* of the purchases, e-mail, texts, phone calls, travel, browsing history, calendar entries, and more on *all* people? The answer to that question is both important and startling. It is important because that degree of data-mining and data-analysis is real and happens every day. It is startling because it means that those who conduct the mining and analysis know everything there is to know about the people whose data they collect and analyze. In fact, since data-analysis uses cold, hard math — instead of emotion — to arrive at conclusions, those who use it know the subjects of surveillance better than those people know themselves.

Perhaps another way of looking at it is this: If Marriott, Target, Facebook, Google, and other companies never collected the personal data in the first place, then hackers could not have stolen the data. No one can steal what does not exist.

*Photo: metamorworks/iStock/Getty Images Plus*