The New York Times

Facebook Isn't Silicon Valley's Only Problem

By Dipayan Ghosh

Mr. Ghosh is a former privacy and public policy adviser at Facebook.

July 2, 2018

Over the past several months, there has been an onslaught of alarming news about Facebook's collection and sharing of users' personal data. The resulting public scrutiny of Facebook is well deserved. But as we scramble to understand the societal harms caused by one Silicon Valley behemoth, we mustn't turn a blind eye to those instigated by the rest of the technology industry.

Facebook is deservedly the most visible public target right now. In March, the whistle-blower Christopher Wylie revealed that the British political advisory firm Cambridge Analytica had illegitimately gained access to more than 50 million people's Facebook data through the efforts of a foreign academic, Aleksandr Kogan. The next month, it was reported that the real number was 87 million. Weeks later, Facebook confirmed that it had entered into many more data partnerships with questionable applications, around 200 of which the company suspended. And last month, it came to light that Facebook has had longstanding data-sharing arrangements with no fewer than 60 manufacturers of device technology, partnerships about which political leaders have expressed deep reservations.

But the reality is that the digital wilderness stretches far beyond Facebook, to a much larger tech ecosystem that deserves holistic examination and, potentially, regulation in the days ahead.

Take, for instance, the industry's widespread but largely nontransparent partnerships with data brokers — companies that are in the business of quietly collecting an enormous amount of sensitive personal data and selling it to whoever will pay for it. Facebook announced recently that it will shut down Partner Categories, the feature that allows data brokers to pipe sensitive information — like your personal interests and behaviors — into Facebook's advertising management system. That allows marketers like Chanel or the N.B.A. to target you with digital ads that they predict you will find relevant. Facebook's pivot was both necessary to protect individual privacy and long overdue.

But the use of data provided by leading data brokers like Acxiom, Experian and Oracle — which typically disclose very little about what kinds of personal data they have and how they use it — is still commonplace across the internet, and most tech companies are willfully uncommunicative

about the nature of their commercial partnerships with data brokers. Digital marketers still purchase access to tools and products provided by data brokers and apply them in ad campaigns on major internet platforms as a matter of everyday business.

You have 3 free articles remaining.
Subscribe to The Times

Consider, too, that most Silicon Valley giants invite third-party developers to create executable programs — like mobile applications and internet-based games — that sit atop their platforms. Facebook recently disclosed that it would be suspending around 200 such partnerships with third-party applications in light of its internal post-Cambridge Analytica investigation. One can only imagine what policies these developers might have breached, but given that the investigation was designed to uncover data misuse, it is likely that they had access to large amounts of Facebook user data and used or shared it without any sort of oversight or restriction.

Facebook's internal review, even if it was undertaken in response to external criticism, is vital to ensure that personal data is not used inappropriately. And that is precisely why we should also take the magnifying glass to Google, Apple and others that similarly partner with vast developer communities that receive special access to inordinate amounts of sensitive user data.

Another example of common practice across the American technology industry is the cultivation of commercial partnerships with foreign companies in ways that present significant national security concerns. Internet companies often make business decisions that cause the United States intelligence community great consternation. Reports about Facebook's data-sharing arrangements with manufacturers were especially alarming because some of them were Chinese companies, including Huawei, which reportedly has close relations with China's government. This raised serious national security concerns: Could the Chinese government have had access to the Facebook data of American citizens? This line of thinking has spurred new inquiries and more policy responses from Facebook — including the recent announcement that it will end its partnership with Huawei.

But Facebook is not the only company that should present such concerns. Just last year, for example, Apple complied with a new Chinese law that required foreign businesses that wish to hold data on Chinese citizens to open a data center in China, enter into commercial partnership with a local Chinese technology company and give the Chinese security authorities access to user data should they demand it — practices that contradict ethical standards.

All internet companies must place humanity first and profits second. The public scrutiny of Facebook has led it to make positive changes in that direction, but we can't forget to hold the broader industry accountable, too.

Dipayan Ghosh is a fellow at the Shorenstein Center at the Harvard Kennedy School and New America. He has served as a technology and economic adviser to the Obama administration and as a United States privacy and public policy adviser at Facebook.

Follow The New York Times Opinion section on Facebook and Twitter (@NYTopinion), and sign up for the Opinion Today newsletter.