As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants

Internal documents show that the social network gave Microsoft, Amazon, Spotify and others far greater access to people's data than it has disclosed.

By Gabriel J.X. Dance, Michael LaForgia and Nicholas Confessore

- Dec. 18, 2018

For years, Facebook gave some of the world's largest technology companies more intrusive access to users' personal data than it has disclosed, effectively exempting those business partners from its usual privacy rules, according to internal records and interviews.

The special arrangements are detailed in hundreds of pages of Facebook documents obtained by The New York Times. The records, generated in 2017 by the company's internal system for tracking partnerships, provide the most complete picture yet of the social network's data-sharing practices. They also underscore how personal data has become the most prized commodity of the digital age, traded on a vast scale by some of the most powerful companies in Silicon Valley and beyond.

The exchange was intended to benefit everyone. Pushing for explosive growth, Facebook got more users, lifting its advertising revenue. Partner companies acquired features to make their products more attractive. Facebook users connected with friends across different devices and websites. But Facebook also assumed extraordinary power over the personal information of its 2.2 billion users — control it has wielded with little transparency or outside oversight.

Facebook allowed Microsoft's Bing search engine to see the names of virtually all Facebook users' friends without consent, the records show, and gave Netflix and Spotify the ability to read Facebook users' private messages.

The social network permitted Amazon to obtain users' names and contact information through their friends, and it let Yahoo view streams of friends' posts as recently as this summer, despite public statements that it had stopped that type of sharing years earlier.

Facebook has been reeling from a series of privacy scandals, set off by revelations in March that a political consulting firm, Cambridge Analytica, improperly used Facebook data to build tools that aided President Trump's 2016 campaign. Acknowledging that it had breached users' trust, Facebook insisted that it had instituted stricter privacy protections long ago. Mark Zuckerberg, the chief executive, assured lawmakers in April that people "have complete control" over everything they share on Facebook.

But the documents, as well as interviews with about 50 former employees of Facebook and its corporate partners, reveal that Facebook allowed certain companies access to data despite those

protections. They also raise questions about whether Facebook ran afoul of a 2011 consent agreement with the Federal Trade Commission that barred the social network from sharing user data without explicit permission.

In all, the deals described in the documents benefited more than 150 companies — most of them tech businesses, including online retailers and entertainment sites, but also automakers and media organizations. Their applications sought the data of hundreds of millions of people a month, the records show. The deals, the oldest of which date to 2010, were all active in 2017. Some were still in effect this year.

In an interview, Steve Satterfield, Facebook's director of privacy and public policy, said none of the partnerships violated users' privacy or the F.T.C. agreement. Contracts required the companies to abide by Facebook policies, he added.

Still, Facebook executives have acknowledged missteps over the past year. "We know we've got work to do to regain people's trust," Mr. Satterfield said. "Protecting people's information requires stronger teams, better technology and clearer policies, and that's where we've been focused for most of 2018." He said that the partnerships were "one area of focus" and that Facebook was in the process of winding many of them down.

Facebook has found no evidence of abuse by its partners, a spokeswoman said. Some of the largest partners, including Amazon, Microsoft and Yahoo, said they had used the data appropriately, but declined to discuss the sharing deals in detail. Facebook did say that it had mismanaged some of its partnerships, allowing certain companies' access to continue long after they had shut down the features that required the data.

With most of the partnerships, Mr. Satterfield said, the F.T.C. agreement did not require the social network to secure users' consent before sharing data because Facebook considered the partners extensions of itself — service providers that allowed users to interact with their Facebook friends. The partners were prohibited from using the personal information for other purposes, he said. "Facebook's partners don't get to ignore people's privacy settings."

Data privacy experts disputed Facebook's assertion that most partnerships were exempted from the regulatory requirements, expressing skepticism that businesses as varied as device makers, retailers and search companies would be viewed alike by the agency. "The only common theme is that they are partnerships that would benefit the company in terms of development or growth into an area that they otherwise could not get access to," said Ashkan Soltani, former chief technologist at the F.T.C.

Mr. Soltani and three former employees of the F.T.C.'s consumer protection division, which brought the case that led to the consent decree, said in interviews that its data-sharing deals had probably violated the agreement.

"This is just giving third parties permission to harvest data without you being informed of it or giving consent to it," said David Vladeck, who formerly ran the F.T.C.'s consumer protection

bureau. “I don’t understand how this unconsented-to data harvesting can at all be justified under the consent decree.”

Details of the agreements are emerging at a pivotal moment for the world’s largest social network. Facebook has been hammered with questions about its data sharing from lawmakers and regulators in the United States and Europe. The F.T.C. this spring opened a new inquiry into Facebook’s compliance with the consent order, while the Justice Department and Securities and Exchange Commission are also investigating the company.

Facebook’s stock price has fallen, and a group of shareholders has called for Mr. Zuckerberg to step aside as chairman. Shareholders also have filed a lawsuit alleging that executives failed to impose effective privacy safeguards. Angry users started a #DeleteFacebook movement.

This month, a British parliamentary committee investigating internet disinformation released internal Facebook emails, seized from the plaintiff in another lawsuit against Facebook. The messages disclosed some partnerships and depicted a company preoccupied with growth, whose leaders sought to undermine competitors and briefly considered selling access to user data.

As Facebook has battled one crisis after another, the company’s critics, including some former advisers and employees, have singled out the data-sharing as cause for concern.

“I don’t believe it is legitimate to enter into data-sharing partnerships where there is not prior informed consent from the user,” said Roger McNamee, an early investor in Facebook. “No one should trust Facebook until they change their business model.”

An Engine for Growth

Personal data is the oil of the 21st century, a resource worth billions to those who can most effectively extract and refine it. American companies alone are expected to spend close to $20 billion by the end of 2018 to acquire and process consumer data, according to the Interactive Advertising Bureau.

Few companies have better data than Facebook and its rival, Google, whose popular products give them an intimate view into the daily lives of billions of people — and allow them to dominate the digital advertising market.

Facebook has never sold its user data, fearful of user backlash and wary of handing would-be competitors a way to duplicate its most prized asset. Instead, internal documents show, it did the next best thing: granting other companies access to parts of the social network in ways that advanced its own interests.

Facebook began forming data partnerships when it was still a relatively young company. Mr. Zuckerberg was determined to weave Facebook’s services into other sites and platforms, believing it would stave off obsolescence and insulate Facebook from competition. Every corporate partner that integrated Facebook data into its online products helped drive the platform’s expansion, bringing in new users, spurring them to spend more time on Facebook and

driving up advertising revenue. At the same time, Facebook got critical data back from its partners.

The partnerships were so important that decisions about forming them were vetted at high levels, sometimes by Mr. Zuckerberg and Sheryl Sandberg, the chief operating officer, Facebook officials said. While many of the partnerships were announced publicly, the details of the sharing arrangements typically were confidential.

By 2013, Facebook had entered into more such partnerships than its midlevel employees could easily track, according to interviews with two former employees. (Like the more than 30 other former employees interviewed for this article, they spoke on the condition of anonymity because they had signed nondisclosure agreements or still maintained relationships with top Facebook officials.)

So they built a tool that did the technical work of turning special access on and off and also kept records on what are known internally as "capabilities" — the special privileges enabling companies to obtain data, in some cases without asking permission.

The Times reviewed more than 270 pages of reports generated by the system — records that reflect just a portion of Facebook's wide-ranging deals. Among the revelations was that Facebook obtained data from multiple partners for a controversial friend-suggestion tool called "People You May Know."

The feature, introduced in 2008, continues even though some Facebook users have objected to it, unsettled by its knowledge of their real-world relationships. Gizmodo and other news outlets have reported cases of the tool's recommending friend connections between patients of the same psychiatrist, estranged family members, and a harasser and his victim.

Facebook, in turn, used contact lists from the partners, including Amazon, Yahoo and the Chinese company Huawei — which has been flagged as a security threat by American intelligence officials — to gain deeper insight into people's relationships and suggest more connections, the records show.

Some of the access deals described in the documents were limited to sharing non-identifying information with research firms or enabling game makers to accommodate huge numbers of players. These raised no privacy concerns. But agreements with about a dozen companies did. Some enabled partners to see users' contact information through their friends — even after the social network, responding to complaints, said in 2014 that it was stripping all applications of that power.

As of 2017, Sony, Microsoft, Amazon and others could obtain users' email addresses through their friends.

Facebook also allowed Spotify, Netflix and the Royal Bank of Canada to read, write and delete users' private messages, and to see all participants on a thread — privileges that appeared to go beyond what the companies needed to integrate Facebook into their systems, the records show.

Facebook acknowledged that it did not consider any of those three companies to be service providers. Spokespeople for Spotify and Netflix said those companies were unaware of the broad powers Facebook had granted them. A Royal Bank of Canada spokesman disputed that the bank had any such access.

Spotify, which could view messages of more than 70 million users a month, still offers the option to share music through Facebook Messenger. But Netflix and the Canadian bank no longer needed access to messages because they had deactivated features that incorporated it.

These were not the only companies that had special access longer than they needed it. Yahoo, The Times and others could still get Facebook users' personal information in 2017.

Yahoo could view real-time feeds of friends' posts for a feature that the company had ended in 2011. A Yahoo spokesman declined to discuss the partnership in detail but said the company did not use the information for advertising. The Times — one of nine media companies named in the documents — had access to users' friend lists for an article-sharing application it also had discontinued in 2011. A spokeswoman for the news organization said it was not obtaining any data.

Facebook's internal records also revealed more about the extent of sharing deals with over 60 makers of smartphones, tablets and other devices, agreements first reported by The Times in June.

Facebook empowered Apple to hide from Facebook users all indicators that its devices were asking for data. Apple devices also had access to the contact numbers and calendar entries of people who had changed their account settings to disable all sharing, the records show.

Apple officials said they were not aware that Facebook had granted its devices any special access. They added that any shared data remained on the devices and was not available to anyone other than the users.

Facebook officials said the company had disclosed its sharing deals in its privacy policy since 2010. But the language in the policy about its service providers does not specify what data Facebook shares, and with which companies. Mr. Satterfield, Facebook's privacy director, also said its partners were subject to "rigorous controls."

Yet Facebook has an imperfect track record of policing what outside companies do with its user data. In the Cambridge Analytica case, a Cambridge University psychology professor created an application in 2014 to harvest the personal data of tens of millions of Facebook users for the consulting firm.

Pam Dixon, executive director of the World Privacy Forum, a nonprofit privacy research group, said that Facebook would have little power over what happens to users' information after sharing it broadly. "It travels," Ms. Dixon said. "It could be customized. It could be fed into an algorithm and decisions could be made about you based on that data."

400 Million Exposed

Unlike Europe, where social media companies have had to adapt to stricter regulation, the United States has no general consumer privacy law, leaving tech companies free to monetize most kinds of personal information as long as they don't mislead their users. The F.T.C., which regulates trade, can bring enforcement actions against companies that deceive their customers.

Besides Facebook, the F.T.C. has consent agreements with Google and Twitter stemming from alleged privacy violations.

Facebook's agreement with regulators is a result of the company's early experiments with data sharing. In late 2009, it changed the privacy settings of the 400 million people then using the service, making some of their information accessible to all of the internet. Then it shared that information, including users' locations and religious and political leanings, with Microsoft and other partners.

Facebook called this "instant personalization" and promoted it as a step toward a better internet, where other companies would use the information to customize what people saw on sites like Bing. But the feature drew complaints from privacy advocates and many Facebook users that the social network had shared the information without permission.

The F.T.C. investigated and in 2011 cited the privacy changes as a deceptive practice. Caught off guard, Facebook officials stopped mentioning instant personalization in public and entered into the consent agreement.

Under the decree, the social network introduced a "comprehensive privacy program" charged with reviewing new products and features. It was initially overseen by two chief privacy officers, their lofty title an apparent sign of Facebook's commitment. The company also hired PricewaterhouseCoopers to assess its privacy practices every two years.

But the privacy program faced some internal resistance from the start, according to four former Facebook employees with direct knowledge of the company's efforts. Some engineers and executives, they said, considered the privacy reviews an impediment to quick innovation and growth. And the core team responsible for coordinating the reviews — numbering about a dozen people by 2016 — was moved around within Facebook's sprawling organization, sending mixed signals about how seriously the company took it, the ex-employees said.

Critically, many of Facebook's special sharing partnerships were not subject to extensive privacy program reviews, two of the former employees said. Executives believed that because the partnerships were governed by business contracts requiring them to follow Facebook data policies, they did not require the same level of scrutiny. The privacy team had limited ability to review or suggest changes to some of those data-sharing agreements, which had been negotiated by more senior officials at the company.

Facebook officials said that members of the privacy team had been consulted on the sharing agreements, but that the level of review "depended on the specific partnership and the time it was created."

In 2014, Facebook ended instant personalization and walled off access to friends' information. But in a previously unreported agreement, the social network's engineers continued allowing Bing; Pandora, the music streaming service; and Rotten Tomatoes, the movie and television review site, access to much of the data they had gotten for the discontinued feature. Bing had access to the information through last year, the records show, and the two other companies did as of late summer, according to tests by The Times.

Facebook officials said the data sharing did not violate users' privacy because it allowed access only to public data — though that included data that the social network had made public in 2009. They added that the social network made a mistake in allowing the access to continue for the three companies, but declined to elaborate. Spokeswomen for Pandora and Rotten Tomatoes said the businesses were not aware of any special access.

Facebook also declined to discuss the other capabilities Bing was given, including the ability to see all users' friends.

Microsoft officials said that Bing was using the data to build profiles of Facebook users on Microsoft servers. They declined to provide details, other than to say the information was used in "feature development" and not for advertising. Microsoft has since deleted the data, the officials said.

Compliance Questions

For some advocates, the torrent of user data flowing out of Facebook has called into question not only Facebook's compliance with the F.T.C. agreement, but also the agency's approach to privacy regulation.

"There has been an endless barrage of how Facebook has ignored users' privacy settings, and we truly believed that in 2011 we had solved this problem," said Marc Rotenberg, head of the Electronic Privacy Information Center, an online privacy group that filed one of the first complaints about Facebook with federal regulators. "We brought Facebook under the regulatory authority of the F.T.C. after a tremendous amount of work. The F.T.C. has failed to act."

According to Facebook, most of its data partnerships fall under an exemption to the F.T.C. agreement. The company argues that the partner companies are service providers — companies that use the data only "for and at the direction of" Facebook and function as an extension of the social network.

But Mr. Vladeck and other former F.T.C. officials said that Facebook was interpreting the exemption too broadly. They said the provision was intended to allow Facebook to perform the same everyday functions as other companies, such as sending and receiving information over the internet or processing credit card transactions, without violating the consent decree.

When The Times reported last summer on the partnerships with device makers, Facebook used the term "integration partners" to describe BlackBerry, Huawei and other manufacturers that pulled Facebook data to provide social-media-style features on smartphones. All such integration partners, Facebook asserted, were covered by the service provider exemption.

Since then, as the social network has disclosed its data sharing deals with other kinds of businesses — including internet companies such as Yahoo — Facebook has labeled them integration partners, too.

Facebook even recategorized one company, the Russian search giant Yandex, as an integration partner.

Facebook records show Yandex had access in 2017 to Facebook's unique user IDs even after the social network stopped sharing them with other applications, citing privacy risks. A spokeswoman for Yandex, which was accused last year by Ukraine's security service of funneling its user data to the Kremlin, said the company was unaware of the access and did not know why Facebook had allowed it to continue. She added that the Ukrainian allegations "have no merit."

In October, Facebook said Yandex was not an integration partner. But in early December, as The Times was preparing to publish this article, Facebook told congressional lawmakers that it was.

An F.T.C. spokeswoman declined to comment on whether the commission agreed with Facebook's interpretation of the service provider exception, which is likely to figure in the F.T.C.'s ongoing Facebook investigation. She also declined to say whether the commission had ever received a complete list of partners that Facebook considered service providers.

But federal regulators had reason to know about the partnerships — and to question whether Facebook was adequately safeguarding users' privacy. According to a letter that Facebook sent this fall to Senator Ron Wyden, the Oregon Democrat, PricewaterhouseCoopers reviewed at least some of Facebook's data partnerships.

The first assessment, sent to the F.T.C. in 2013, found only "limited" evidence that Facebook had monitored those partners' use of data. The finding was redacted from a public copy of the assessment, which gave Facebook's privacy program a passing grade over all.

Mr. Wyden and other critics have questioned whether the assessments — in which the F.T.C. essentially outsources much of its day-to-day oversight to companies like PricewaterhouseCoopers — are effective. As with other businesses under consent agreements with the F.T.C., Facebook pays for and largely dictated the scope of its assessments, which are limited mostly to documenting that Facebook has conducted the internal privacy reviews it claims it had.

How closely Facebook monitored its data partners is uncertain. Most of Facebook's partners declined to discuss what kind of reviews or audits Facebook subjected them to. Two former

Facebook partners, whose deals with the social network dated to 2010, said they could find no evidence that Facebook had ever audited them. One was BlackBerry. The other was Yandex.

Facebook officials said that while the social network audited partners only rarely, it managed them closely.

“These were high-touch relationships,” Mr. Satterfield said.