Should Facebook shift to private, encrypted communications?

Word Count: 1456 ✓

29 March 2019

Table of Contents

G STRUCTURE

Introduction

FWD LNK

I chose to write my commentary on Facebook CEO Mark Zuckerberg's recent announcement that he will restructure Facebook toward private, encrypted communication. Zuckerberg explained that privacy means groups will evolve into "simple, intimate places," and end-to-end encryption prevents anyone, including Facebook, from reading content (SD 3A). This would be a large change to Facebook's current structure of public groups that are not end-to-end encrypted. I conducted secondary research and compiled a list of source documents I will use to evaluate whether Facebook should follow through with this announcement:

OEA

- Source Document 1: "Facebook's Mark Zuckerberg says he'll reorient the company toward encryption and privacy"
- Source Document 2: "Facebook Says It's Evolving, So What About Its $55 Billion in Ad Sales?"
- Source Document 3 (Zuckerberg's post): "A Privacy-Focused Vision for Social Networking"
- Source Document 4: "Facebook's pivot to privacy has huge implications—if it's real"
- Source Document 5: "Facebook to encrypt Instagram messages ahead of integration with WhatsApp, Facebook Messenger"

BRAND VALUE

Findings and Analysis

INT. LNG. CONTENT

Facebook's proposed overhaul would have several positive effects on its product mix, as shown by its product life cycle. Between 2017 and 2018, usage of Facebook declined by about 10% (SD 1C). This is an alarming trend for the company because the Facebook social network is its core product. Facebook is reaching the end of its maturity stage and is facing saturation in the

CONTENT CONTEXT ASSERTION Application

U.S. market. One reason for this is the record-low public trust in Facebook because of privacy controversies (SD 1B). As a result, Facebook needs an extension strategy to prolong sales revenue. Zuckerberg's announcement proposes the strategy of redesigning. Redesigning Facebook toward privacy and encryption would be important for multiple reasons.

Aplicatn

INT. JUDGMENT

First, it creates a unique selling point—security and intimacy—that is in line with Facebook's earlier efforts to end-to-end encrypt Instagram and Messenger messages (SD 5A). According to Ashkan Soltani, a formal Federal Trade Commission official, "this move is entirely a strategic play to use privacy as a competitive advantage and further lock in Facebook as the dominant messaging platform" (SD 1D). The strategy adds value to the product and differentiates it from rivals in the market. Product differentiation will likely prolong Facebook's product life cycle because of this added value for the user.

I.J.

Second, protecting customer privacy would be an ethical business practice. As Zuckerberg wrote, "encryption is decentralizing—it limits services like [theirs] from seeing the content flowing through them" (SD 3B). People are increasingly aware that encrypting data generally protects their privacy and prevents their data from being misused. Facebook currently has 2.32 billion users (SD 2C). With such a large consumer market, trust and perception are critical. Encrypting all Facebook content would create this trust by showing users that Facebook acts ethically, improving brand image. This is especially important for Facebook because of its shockingly low level of public trust.

I. J.

The Boston Matrix reveals another reason in favor of the shift as well as a major drawback. In the following page is a current Boston Matrix for the company with the four main elements of its product portfolio based on my research.

BAL.

Figure 1: Boston Matrix for Facebook Product Portfolio

		Market Share	
		High	*Low*
Market growth	*High (growing)*	Stars WhatsApp	Question Marks Instagram Rising Stars Messenger
	Low (mature)	Cash Cows Facebook (News Feed)	Dogs

G-DIG

W DEF

As the Boston Matrix shows, WhatsApp is a star. Last year, WhatsApp surpassed Facebook in the number of regular users, and the market continues to grow rapidly (SD 1E). ✓ WhatsApp messages have long been end-to-end encrypted, and they are the model for Facebook's new privacy development. Earlier, Facebook introduced end-to-end encryption to Instagram and Messenger to try to bring it closer to WhatsApp's status as a rising star (SD 5A). ✓ This previous strategy shows the viability of doing the same to the Facebook social network. By modeling Facebook on WhatsApp, the company will likely face a similar market growth and I.J. enjoy the revenue benefits of stars. vague

RM However, the Boston Matrix also demonstrates a significant weakness of the proposed plan. According to analyst Casey Newton, Facebook's News Feed is "the most lucrative advertising product ever built" (SD 4A). ✓ The News Feed is a cash cow; although it is not facing GDEF market growth, it generates high earnings. The News Feed lets users see their friends' public updates at the same time as displaying high-price, personalized ads. If Facebook shifts to private

communications, this important cash cow would decline, becoming a dog. Facebook would lose GA
a key source of its revenue and would have to create a new business model to justify this loss.

This proposed development would have a mostly negative effect on Facebook's revenue. Since the company is so large, the ability to monetize its massive user base should always be considered before a strategy change, or the firm's profitability could be at risk. Facebook makes most of its revenue by mining customer data to create extensive individual customer profiles (SD 1F). For example, Facebook is able to price the News Feed ads so high because the ads can be targeted to specific users based on their profiles. In fact, e-marketer analyst Debra Aho Williamson projected Facebook will make $67 billion in public ad revenue this year (SD 2A). With encrypted content, Facebook would lose valuable customer data, and ad revenue would sharply decrease. Without a new source of revenue, Facebook could face profitability problems after a shift to encryption. In the long term, Facebook would need a new business model to exceed the existing ad revenue, but analysts are unclear about how Facebook can do this I.J.
effectively.

One possible avenue is for the new business model to be e-commerce. Zuckerberg said DEVELOPMENT
that "from the consumer side, increasing commerce on Instagram, Facebook and WhatsApp, I think, is one of the most exciting product opportunities" (SD 2B). It is possible that commerce could replace ads as Facebook's main source of revenue. Already, Instagram is creating a standalone shopping app (SD 4B). However, developing these new products would take enormous amounts of time and resources.

There are also large risks associated with Zuckerberg's announcement in terms of Facebook's global position. These risks can be analyzed with a partial PESTLE analysis of external factors. For political factors, Facebook would be banned in several large countries like

Vietnam and Russia that demand unencrypted data so that their governments can intercept content (SD 4C). This limits Facebook's global market growth and can create conflicts with governments. Socially, the spread of misinformation is a risk associated with encryption. There are certain countries, like India and Brazil, where misinformation is more popular. For example, misinformation in India through WhatsApp has created mobs and fatalities (SD 1A). Since the misinformation cannot be addressed if it is encrypted, encryption in countries prone to misinformation would be problematic. The corresponding legal opportunity, however, is that Facebook would have legal protection for any problems because they cannot read content. Finally, there are ethical considerations. Although encryption protects privacy, this includes protecting the privacy of immoral, dangerous activities like child abuse, extortion, and terrorism. In countries where these are more common, end-to-end encryption could be misused as a harmful weapon. This could harm the company's brand image. The partial PESTLE analysis reveals that shifting to encrypted communications is likely to hurt Facebook's global position. I. J.

The potential change has varying effects on Facebook's many stakeholders. As shown by the PESTLE analysis, two stakeholders the shift would negatively impact are foreign governments and law enforcement. Both of these external groups want unencrypted data because they want to be able to intercept and use the data for their own needs. The other group mainly affected by the decision is the user base. Many users advocate for the change because the increased privacy and security add emotional value by making them feel safer using the product. To assess how to deal with these conflicting viewpoints, the next page has a stakeholder map of key stakeholders for this decision:

Figure 2: Stakeholder Mapping for Facebook Decision

		Level of Interest	
		Low	*High*
Level of Power	*Low*	Minimum effort	Keep informed Law Enforcement Foreign Governments
	High	Keep satisfied	Maximum effort Customers

Foreign governments do have considerable power over Facebook because they can ban the product, but only some governments would do this. Facebook can still survive by operating only in countries that support it. Ultimately, customers have the most direct influence in this decision, so Facebook should put maximum effort to cater to their wants.

Conclusion

After analyzing the effects of Zuckerberg's decision on product portfolio, revenue, global position, and stakeholders, I conclude that Facebook should shift to private, encrypted communications as long as it commits resources to and fully plans out a new business model Judgement based on e-commerce. Although this decision would lead to the obsolescence of the News Feed, the loss of this ad revenue can be offset by focusing on integrating commerce into Facebook's products. This is vital: without commerce revenue to balance lost ad revenue, Facebook will have long-term financial issues that would make it difficult to cope with the lowering in global position in certain countries that comes with encryption. Hence, the ability to introduce e-commerce is a key assumption in this analysis. In the end, the priority for Facebook right now is to satisfy its customers and rebuild trust in order to extend its product life cycle, and Zuckerberg's plan will begin this process.

Works Cited

Dwoskin, Elizabeth. "Facebook's Mark Zuckerberg Says He'll Reorient the Company toward Encryption and Privacy." *The Washington Post*, WP Company, 6 Mar. 2019, www.washingtonpost.com/technology/2019/03/06/facebooks-mark-zuckerberg-says-hell-reorient-company-towards-encryption-privacy/?utm_term=.7be5a378f4c8. Accessed 9 Mar. 2019.

Newton, Casey. "Facebook's pivot to privacy has huge implications—if it's real." *The Verge*, Vox Media, 8 Mar. 2019, www.theverge.com/interface/2019/3/6/18253922/facebook-privacy-meaning-implications-mark-zuckerberg-pivot-analysis-interface-casey-newton.

Swartz, Jon. "Facebook Says It's Evolving, So What About Its $55 Billion in Ad Sales?" *Barron's*, Barrons, 8 Mar. 2019, www.barrons.com/articles/facebook-future-of-advertising-51552066792. Accessed 9 Mar. 2019.

Whittaker, Zack. "Facebook to encrypt Instagram messages ahead of integration with WhatsApp, Facebook Messenger" *Tech Crunch*, Verizon Media, 25 Jan. 2019, https://techcrunch.com/2019/01/25/facebook-instagram-encryption-integration/. Accessed 9 Mar. 2019.

Zuckerberg, Mark. "A Privacy-Focused Vision for Social Networking." *Facebook*, Facebook, 6 Mar. 2019, www.facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634/. Accessed 9 Mar. 2019.

Appendix

Source Document #1: *Facebook's Mark Zuckerberg says he'll reorient the company toward encryption and privacy.* March 6, 2019.

Facebook, which for a generation has encouraged billions of people to widely share their life updates and pictures, is trying to reinvent itself as a place for private communication.

Chief executive Mark Zuckerberg on Wednesday announced a sweeping reorientation toward privacy, explaining in a lengthy essay posted to his account that he would spend the coming years focusing the company's distinct apps — WhatsApp, Instagram, Messenger, and Facebook — on content that is encrypted, meaning data is scrambled so that outsiders, and even Facebook, cannot read it. But the shift, which shows how the embattled company is positioning itself for an uncertain future marked by consumer distrust, declining growth on its core social network and ongoing fights with regulators around the world, could cause an upheaval in Facebook's business model of mining people's information to show them ads.

While offering few specifics, Zuckerberg said the company would move from being a social network where people broadcast information to large groups — a town hall — to a service that is modeled after a living room, where people communicate with smaller, trusted groups.

"As I think about the future of the internet, I believe a privacy-focused communications platform will become even more important than today's open platforms," Zuckerberg wrote. "Privacy gives people the freedom to be themselves and connect more naturally, which is why we build social networks."

Reactions to Zuckerberg's announcement were swift and skeptical. Privacy advocates said Zuckerberg needs to go beyond touting encryption to provide concrete information about whether less data will be collected and used for Facebook's profits. "Why does it always sound like we are witnessing a digital version of Groundhog Day when Facebook yet again promises — when it's in a crisis — that it will do better," said Jeff Chester, executive director of the Center for Digital Democracy, a nonprofit privacy advocacy group in Washington. "Will it actually bring a change to how Facebook continually gathers data on its users in order to drive big profits?"

The promised shift to more secure communications, while good for users, could entail major risks to Facebook's global position. Many governments oppose encryption, and Zuckerberg acknowledged Facebook may end up getting blocked in some foreign countries as a result. Encryption will also make it harder for Facebook to fulfill what Zuckerberg has described as a core mission of detecting misinformation operatives and other bad actors on the company's platform, which requires the ability to read the content people post. On Twitter, Facebook's former chief security officer Alex Stamos said law enforcement and people who care about moderating unwanted content were the "losers" of Wednesday's announcement.

Jennifer Grygiel, assistant professor of communications at Syracuse University, said Facebook's changes would severely curtail its ability to moderate content. "What's not clear is how they are going to make this transition safely. We have already seen the risks associated with WhatsApp and private
A encryption in India, for example, where misinformation has led to mobs and the loss of life," she said.

B Public trust in Facebook is at record lows, according to studies, the result of crushing privacy controversies last year as well as the misuse of user data that extends back more than a decade. In a reputation score of 100 highly visible public companies, Facebook last year dropped from 51st to 94th, according to a Harris Poll published Wednesday in conjunction with the news organization Axios. In a Pew Research Center study from September, a quarter of the Facebook users polled said they deleted the app from their smartphones last year, and more than half said they adjusted their privacy settings.

Zuckerberg acknowledged the trust deficit in his post. "I understand that many people don't think Facebook can or would even want to build this kind of privacy-focused platform — because frankly we don't currently have a strong reputation for building privacy protective services, and we've historically focused on tools for more open sharing," he wrote. "But we've repeatedly shown that we can evolve to build the services that people really want, including in private messaging and stories."

But the moves also appear to be prompted by business considerations. Since 2012, Facebook has grown from a single social network, Facebook, to what Zuckerberg refers to as a "family" of four apps, with Messenger, Instagram and WhatsApp. Facebook was long the star, but last year
E WhatsApp surpassed it in the number of people who use it on a monthly basis, according to industry reports. Zuckerberg recently began emphasizing the number of people who use at least one of its products once a month — 2.7 billion people — over the 2.3 billion monthly users for Facebook alone. Users log on to messaging apps more frequently than the core social network, whose growth has flattened in the United States and Europe.

C Usage of Facebook and of Messenger in the United States also appear to have declined by about 10 percent per person between 2017 and 2018, according to Brian Wieser, an analyst with Pivotal Research Group. The trend is worrisome for Facebook because U.S. users on the core social network are the most lucrative, as Facebook can command high ad prices to target them.

D "This move is entirely a strategic play to use privacy as a competitive advantage and further lock in Facebook as the dominant messaging platform," Ashkan Soltani, a former Federal Trade Commission official and privacy researcher, said on Twitter.

Zuckerberg's new blueprint for Facebook arrives as regulators around the world, including the United States, are forging ahead with efforts to craft new rules targeting how companies collect and monetize their users' data. There is widespread trepidation that tech giants know too much about their users — and immense frustration that Facebook in particular has failed to safeguard that data from abuse.

Facebook's mishaps have triggered an investigation from the Federal Trade Commission, which is considering a multibillion-dollar fine against the social networking company. Facebook also is set to defend itself against a lawsuit Wednesday filed by D.C. attorney general, who alleged the company deceived its users about its data-collection practices.

But some of the ideas Zuckerberg has proposed could result in their own share of regulatory headaches. Already, European officials have criticized Facebook for its plan to merge communications services after initially promising to keep apps including WhatsApp separate, and greater integration between Facebook's apps may raise antitrust concerns.

Zuckerberg has routinely reaffirmed Facebook's commitment to privacy when apologizing for scandals. But the difference in Wednesday's announcement were the structural changes Zuckerberg said he intends to make to Facebook's wide array of services — changes that he said he hopes will ensure that Facebook, with its damaged reputation and slowed growth, has a place in the future of social media.

WhatsApp, which Facebook acquired for $19 billion in 2014, is the model for Facebook's new embrace of privacy. While WhatsApp has been end-to-end encrypted for years, Facebook's stand-alone Messenger app is not. Messaging within Facebook's Instagram app is also not encrypted.

In Zuckerberg's blog, he set out a vision for "interoperability," meaning that the changes would not only make messaging more private, they would allow people to message and communicate with one another across the company's apps.

More fluid communication could also help Facebook achieve a goal that so far it has made little progress on: making money off its messaging platforms. Messaging apps, while hugely popular with users, generate a fraction of the revenue compared with the core social network. The company recently introduced advertising on Messenger and also allows businesses to pay to reach customers on WhatsApp.

F But Facebook makes the vast majority of its revenue by targeting ads to U.S. and European users of its core social network, and Zuckerberg didn't address the revenue implications of the privacy shift. Facebook can command the highest ad prices to target these groups because the company has extensive profiles of them and they make the most purchases. If the company cannot read the content of messages, it will lose valuable profiling data.

If Zuckerberg continues to encrypt more services, Facebook could run into more trouble internationally.

WhatsApp's encryption has gotten the service into bruising fights with governments in India and Brazil, two of Facebook's largest markets. Brazil has shut down WhatsApp on three different occasions when government officials asked for data that WhatsApp said it did not have. The Indian government has also proposed breaking WhatsApp's encryption to make the data in it more traceable [...]

Source Document #2: *Facebook Says It's Evolving, So What About Its $55 Billion in Ad Sales?* March 8, 2019.

Mark Zuckerberg used 3,000 words this week to outline his new strategy for Facebook 's privacy plan. Surprisingly, very few of them were about advertising. In fact, he mentioned the advertising word only twice in his lengthy blog post, despite the fact that ads represented the bulk of Facebook's $56 billion in revenue last year.

The word choice left some wondering if Facebook had a real plan to monetize its shifting focus toward private communications.

"This move could have an enormous impact on Facebook's advertising business," eMarketer analyst Debra Aho Williamson told Barron's in an email message.

A

Williamson estimates Facebook (ticker: FB) will generate over $67 billion in ad revenue world-wide this year, with a vast majority of ads appearing in news feeds and other public posts—not private communications.

"Facebook so far has not gained much traction with advertising in Messenger, and advertising in WhatsApp still hasn't emerged," she said. "That creates huge unknowns about how Facebook will generate significant ad revenue while users are engaged in private communications."

Forrester analyst Jessica Liu was equally blunt in a blog post. "Zuckerberg can't have his cake and eat it, too: He is trying to strike an impossible balance between growing users and time spent in-app to fuel more advertising dollars, while also trying to build a singular 'privacy-first experience' to appease privacy regulators, all under a cloud of potential anti-competition breakups," she wrote.

C

By proposing to split Facebook into public and private spaces, Zuckerberg set off alarms among analysts and investors about how the company can continue to monetize its massive user base, which was 2.32 billion at last count.

But any worries are likely exaggerated, says Brian Wieser, a former Wall Street analyst who recently became head of business intelligence for GroupM, WPP's ad buying unit.

"It's too early to say," Wieser told Barron's. "If Facebook decides to nudge consumers more to privacy messaging, it could have an impact on public content and advertising. But we don't know yet."

A Facebook spokesman declined to comment when pressed for details about what the business shift meant for ad revenue. "Nothing to add beyond what Mark covered in his post," he said in an email.

The continuing privacy concerns and questions about data use, have weighed on Facebook's reputation over the last year and its perception with at least some users.

A survey released Thursday showed diminished time spent on Facebook in the fourth quarter of 2018 among a panel of 4,000 Android users, according to AppOptix, a division of research firm Strategy

Analytics. The decline was more pronounced among millennials, who opted for video-heavy services such as Instagram and Alphabet 's (GOOG) YouTube.

But you'd be hard pressed to find any evidence of eroding ad sales and revenue at the social-networking behemoth. Facebook shares are up 29% this year—as is revenue, which soared 30% to $16.91 billion in the company's recently completed fiscal fourth quarter.

Those numbers just raise the stakes as Zuckerberg begins to talk about Facebook's mission in a new way. The CEO's manifesto portends new businesses in the form of private, secure messaging platforms with encryption for financial transactions, according to tech executives, advertising experts, and industry analysts.

With an estimated 1.5 billion users, including 200 million in India, WhatsApp is the world's biggest messaging platform. Instagram has over 1 billion monthly active users. Facebook doesn't break out their revenue.

"Facebook was already headed in this direction: It had to figure out a way to monetize WhatsApp, which it spent over $20 billion on," Justin Choi, CEO of advertising-technology platform Nativo, told Barron's in a phone interview.

Choi says that Zuckerberg's blog post was able to lay the groundwork for what it plans to do with WhatsApp, reassure customers concerned about their personal information, and make a conciliatory political statement to lawmakers and regulators who are threatening privacy legislation. (Facebook is bracing for a record fine from the Federal Trade Commission over its handling of the Cambridge Analytica scandal last year. On Friday, Sen. Elizabeth Warren named Facebook in her new plan to break up big tech companies.)

Highlighting privacy-focused properties such as WhatsApp, Instagram, and Messenger under a "unified messaging platform" would create a "totally different business" rivaling WeChat , Alibaba (BABA), and PayPal 's (PYPL) Venmo for secure transactions, Scott Swanson, CEO of mobile-marketing company Aki Technologies, told Barron's in a phone interview.

Forrester analyst Thomas Husson explained Zuckerberg had no choice but to re-establish trust with its 2.32 billion monthly active users.

"Facebook is entering a transition phase where it will continue to sell targeted ads on its public social networks, while inventing a new business model" between consumers and brands, Husson said in an email.

During Facebook's first-quarter report on Jan. 30, the company said payments and other fees revenue, which include peer-to-peer transactions and online game purchases, increased 42% year over year to $274 million.

B

That day, on a conference call with analysts, Zuckerberg said: "When I think about it, just from the consumer side, increasing commerce on Instagram, Facebook and WhatsApp, I think, is one of the most exciting product opportunities that we have in all of these products and a big business opportunity as well."

Source Document #3 (Zuckerberg's post): *A Privacy-Focused Vision for Social Networking.* March 6, 2019.

[...] This privacy-focused platform will be built around several principles:

A
Private interactions. People should have simple, intimate places where they have clear control over who can communicate with them and confidence that no one else can access what they share.
Encryption. People's private communications should be secure. End-to-end encryption prevents anyone -- including us -- from seeing what people share on our services.
Reducing Permanence. People should be comfortable being themselves, and should not have to worry about what they share coming back to hurt them later. So we won't keep messages or stories around for longer than necessary to deliver the service or longer than people want them.
Safety. People should expect that we will do everything we can to keep them safe on our services within the limits of what's possible in an encrypted service.
Interoperability. People should be able to use any of our apps to reach their friends, and they should be able to communicate across networks easily and securely.
Secure data storage. People should expect that we won't store sensitive data in countries with weak records on human rights like privacy and freedom of expression in order to protect data from being improperly accessed.

Over the next few years, we plan to rebuild more of our services around these ideas. The decisions we'll face along the way will mean taking positions on important issues concerning the future of the internet. We understand there are a lot of tradeoffs to get right, and we're committed to consulting with experts and discussing the best way forward. This will take some time, but we're not going to develop this major change in our direction behind closed doors. We're going to do this as openly and collaboratively as we can because many of these issues affect different parts of society.

Private Interactions as a Foundation

For a service to feel private, there must never be any doubt about who you are communicating with. We've worked hard to build privacy into all our products, including those for public sharing. But one great property of messaging services is that even as your contacts list grows, your individual threads and groups remain private. As your friends evolve over time, messaging services evolve gracefully and remain intimate.

This is different from broader social networks, where people can accumulate friends or followers until the services feel more public. This is well-suited to many important uses -- telling all your friends about something, using your voice on important topics, finding communities of people with similar interests, following creators and media, buying and selling things, organizing fundraisers, growing businesses, or many other things that benefit from having everyone you know in one place. Still, when you see all these experiences together, it feels more like a town square than a more intimate space like a living room.

There is an opportunity to build a platform that focuses on all of the ways people want to interact privately. This sense of privacy and intimacy is not just about technical features -- it is designed deeply into the feel of the service overall. In WhatsApp, for example, our team is obsessed with creating an intimate environment in every aspect of the product. Even where we've built features that allow for broader sharing, it's still a less public experience. When the team built groups, they put in a size limit to make sure every interaction felt private. When we shipped stories on WhatsApp, we limited public content because we worried it might erode the feeling of privacy to see lots of public content -- even if it didn't actually change who you're sharing with.

In a few years, I expect future versions of Messenger and WhatsApp to become the main ways people communicate on the Facebook network. We're focused on making both of these apps faster, simpler, more private and more secure, including with end-to-end encryption. We then plan to add more ways to interact privately with your friends, groups, and businesses. If this evolution is successful, interacting with your friends and family across the Facebook network will become a fundamentally more private experience.

Encryption and Safety

People expect their private communications to be secure and to only be seen by the people they've sent them to -- not hackers, criminals, over-reaching governments, or even the people operating the services they're using.

There is a growing awareness that the more entities that have access to your data, the more vulnerabilities there are for someone to misuse it or for a cyber attack to expose it. There is also a growing concern among some that technology may be centralizing power in the hands of governments and companies like ours. And some people worry that our services could access their messages and use them for advertising or in other ways they don't expect.

End-to-end encryption is an important tool in developing a privacy-focused social network.

B Encryption is decentralizing -- it limits services like ours from seeing the content flowing through them and makes it much harder for anyone else to access your information. This is why encryption is an increasingly important part of our online lives, from banking to healthcare services. It's also why we built end-to-end encryption into WhatsApp after we acquired it.

In the last year, I've spoken with dissidents who've told me encryption is the reason they are free, or even alive. Governments often make unlawful demands for data, and while we push back and fight these requests in court, there's always a risk we'll lose a case -- and if the information isn't encrypted we'd either have to turn over the data or risk our employees being arrested if we failed to comply. This may seem extreme, but we've had a case where one of our employees was actually jailed for not providing access to someone's private information even though we couldn't access it since it was encrypted.

At the same time, there are real safety concerns to address before we can implement end-to-end encryption across all of our messaging services. Encryption is a powerful tool for privacy, but that includes the privacy of people doing bad things. When billions of people use a service to connect, some of them are going to misuse it for truly terrible things like child exploitation, terrorism, and extortion. We have a responsibility to work with law enforcement and to help prevent these wherever we can. We are working to improve our ability to identify and stop bad actors across our apps by detecting patterns of activity or through other means, even when we can't see the content of the messages, and we will continue to invest in this work. But we face an inherent tradeoff because we will never find all of the potential harm we do today when our security systems can see the messages themselves.

Finding the right ways to protect both privacy and safety is something societies have historically grappled with. There are still many open questions here and we'll consult with safety experts, law enforcement and governments on the best ways to implement safety measures. We'll also need to work together with other platforms to make sure that as an industry we get this right. The more we can create a common approach, the better.

On balance, I believe working towards implementing end-to-end encryption for all private communications is the right thing to do. Messages and calls are some of the most sensitive private conversations people have, and in a world of increasing cyber security threats and heavy-handed government intervention in many countries, people want us to take the extra step to secure their most private data. That seems right to me, as long as we take the time to build the appropriate safety systems that stop bad actors as much as we possibly can within the limits of an encrypted service. We've started working on these safety systems building on the work we've done in WhatsApp, and we'll discuss them with experts through 2019 and beyond before fully implementing end-to-end encryption. As we learn more from those experts, we'll finalize how to roll out these systems [...]

Source Document #4: *Facebook's pivot to privacy has huge implications — if it's real.* March 8, 2019.

[...] But say you take Zuckerberg at his word. Say Facebook pivots to privacy, investing most of its energy into groups and messaging products. If that becomes true, then what else is true?

The News Feed becomes a legacy product. Since its introduction, the endless scroll of updates from your friends has been the core of Facebook — synonymous with the experience of using the app itself. Zuckerberg just told the world that he expects it to slowly fade away — not without its uses, but no longer the center of all social media. This could have implications that extend well beyond Facebook proper — to Instagram, for example, and to Twitter.

A **Facebook has to find a new business model**. The News Feed is more than just Facebook's core consumer product — it's the company's core business unit. The News Feed is, along with Google's

AdWords, the most lucrative advertising product ever built. A world in which it withers away is one in which Facebook has to first replace, than exceed the revenues it currently generates from advertising. It will be a Herculean task.

B

That new business model will probably be commerce. Commerce and payments all the rage inside Facebook these days. On the commerce side, Instagram is spinning up a standalone shopping app. On the payments front, David Marcus' team is developing a cryptocurrency. In his blog post, Zuckerberg says a more private suite of Facebook services will give rise to "businesses, payments, commerce, and ultimately a platform for many other kinds of private services."

Regulators will have to make a choice. Lawmakers in some countries have expressed concern about a central element of Zuckerberg's plan, which is to unify the back-end technologies powering Messenger, Instagram, and WhatsApp. Among other things, the move makes it harder for the Federal Trade Commission to order Facebook to spin off one or both of the latter two acquisitions. The question is whether they might allow the unification to go through in exchange for more robust privacy protections and a new business model that is less reliant on personal data. (This is a stretch! All of this is a stretch!)

C

Facebook will be banned in large countries. Countries including Russia and Vietnam are increasingly demanding that tech platforms store user data locally, where it is more easily intercepted by law enforcement agencies. The pivot to privacy doesn't square with those laws, and could have significant consequences. Zuckerberg seems resigned to this fate:

"Upholding this principle may mean that our services will get blocked in some countries, or that we won't be able to enter others anytime soon," Zuckerberg writes. "That's a tradeoff we're willing to make. We do not believe storing people's data in some countries is a secure enough foundation to build such important internet infrastructure on."

Facebook will never open for business in China. Ryan Mac has a senior Facebook official saying that this is, in fact, the case.

Facebook will find itself increasingly at odds with law enforcement. People plan terrorism and other crimes using encrypted messaging apps, and in Facebook's encrypted future, we can expect law enforcement agencies around the world to make great hay out of Facebook's complicity. If I'm on Facebook's communications team, I would actually see this as a good thing: Facebook standing up for its users in the face of pressure from, say, the FBI might help change public sentiment around who has their back, regardless of the particulars of the case. (I hasten to add that terrorism is bad and I hope that no one uses WhatsApp to plan it!)

Misinformation will become harder to track. WhatsApp is already a huge source of misinformation in countries where it is popular, most notably India and Brazil. Shifting more public conversation to encrypted private spaces will mean we have less visibility into public sentiment — and, potentially, how politics are being played by candidates and interest groups. It's tradeoffs all the way down.

If you work at Facebook, all this would represent an extraordinary amount of change. It is not, exactly, unprecedented; one reader likened it to Microsoft's announcement in 2002 that it would put privacy and security ahead of new feature development, after enduring years of criticism over security failures. But it's still likely to be quite messy.

All that said: it could have real benefits, too, especially to normal people who just want to text friends, family, and co-workers, and not have it come back to haunt them. (Or have those messages used to target ads at them, in the way Messenger currently does.) This was Snapchat's original insight, and Facebook is still learning it all these years later.

Zuckerberg is fond of grand pronouncements — it's less than four years since he declared that the News Feed would one day primarily be video, and just two years since he announced that Facebook would concentrate on "developing social infrastructure," whatever that might have meant. In any case, neither vision came true. Whether this one does, facing even longer odds, remains anyone's guess.

Source Document #5: *Facebook to encrypt Instagram messages ahead of integration with WhatsApp, Facebook Messenger*. January 25, 2019.

Facebook is planning to roll out end-to-end encryption for Instagram messages, as part of a broader integration effort across the company's messaging platforms, including **WhatsApp** and Facebook Messenger.

First reported by The New York Times, the social media giant said reworking the underlying infrastructure of its three messaging apps will allow users to talk to each other more easily. The apps will reportedly remain independent of one another — with Instagram and WhatsApp bringing in 1 billion and 1.5 billion users, respectively.

In doing so, Facebook is adding end-to-end encryption to Instagram messages. That will bring a new level of security and privacy to Instagram users for the first time. Facebook will also begin encrypting Facebook Messenger by default, which has, to date, required users to manually switch on the feature.

A

So far, only WhatsApp messages are end-to-end encrypted by default.

The plans are part of the company's effort to keep people on the platform for longer, the Times reported, at a time when the company has 2.2 billion users but user trust has declined following a string of privacy scandals and security incidents. End-to-end encrypted messages can't be read beyond the sender and the recipient — not even Facebook. In shutting itself out of the loop, it reduces the amount of data it can access — and can be theoretically stolen by hackers.

"We want to build the best messaging experiences we can; and people want messaging to be fast, simple, reliable and private," a Facebook spokesperson told TechCrunch. "We're working on making more of our messaging products end-to-end encrypted and considering ways to make it easier to reach friends and family across networks."

"As you would expect, there is a lot of discussion and debate as we begin the long process of figuring out all the details of how this will work," the spokesperson said, without providing a timeline on the planned unification.

But how the integration will be met by European regulators is anybody's guess.

Two years ago, Facebook rolled back its plans to begin sharing WhatsApp user data with the social network for advertising at the request of U.K. data protection authorities, putting the plan on ice across the European continent. Under the proposed changes to its terms and conditions, WhatsApp would have shared the user's phone number that was used to verify their account, and the last time they used the service. That led to concerns about privacy, given that a real-world identity isn't needed for WhatsApp, unlike Facebook, which requires users display their real names.

Facebook acknowledged that it didn't have answers just yet about how it plans to navigate the issue, citing the early stages of its planned integration [...]