Luxury Daily®

The News and Intelligence You Need on Luxury

MEDIA/PUBLISHING

Facebook's Mark Zuckerberg: A privacy-focused vision for social networking

March 7, 2019

Facebook's future: All locked up? Image credit: Facebook

By Mark Zuckerberg

Subscribe to Luxury Daily
Plus: Just released State of Luxury 2019
Save $246

My focus for the last couple of years has been understanding and addressing the biggest challenges facing Facebook. This means taking positions on important issues concerning the future of the Internet. In this note, I'll outline our vision and principles around building a privacy-focused messaging and social networking platform. There's a lot to do here, and we're committed to working openly and consulting with experts across society as we develop this.

Over the last 15 years, Facebook and Instagram have helped people connect with friends, communities, and interests in the digital equivalent of a town square. But people increasingly also want to connect privately in the digital equivalent of the living room. 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. Privacy gives people the freedom to be themselves and connect more naturally, which is why we build social networks.

Today we already see that private messaging, ephemeral stories, and small groups are by far the fastest growing areas of online communication. There are a number of reasons for this. Many people prefer the intimacy of communicating one-on-one or with just a few friends. People are more cautious of having a permanent record of what they've shared. And we all expect to be able to do things like payments privately and securely.

Public social networks will continue to be very important in people's lives – for connecting with everyone you know, discovering new people, ideas and content, and giving people a voice more broadly. People find these valuable every day, and there are still a lot of useful services to build on top of them. But now, with all the ways people also want to interact privately, there's also an opportunity to build a simpler platform that's focused on privacy first.

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. But we've repeatedly shown that we can evolve to build the services that people really want, including in private messaging and stories.

Mark Zuckerberg is cofounder/CEO of Facebook. Image credit: Mark Zuckerberg, Twitter

I believe the future of communication will increasingly shift to private, encrypted services where people can be confident what they say to each other stays secure and their messages and content won't stick around forever. This is the future I hope we will help bring about.

We plan to build this the way we've developed WhatsApp: focus on the most fundamental and private use case – messaging – make it as secure as possible, and then build more ways for people to interact on top of that, including calls, video chats, groups, stories, businesses, payments, commerce, and ultimately a platform for many other kinds of private services.

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

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. 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.

Reducing Permanence

We increasingly believe it's important to keep information around for shorter periods of time. People want to know that what they share won't come back to hurt them later, and reducing the length of time their information is stored and accessible will help.

One challenge in building social tools is the "permanence problem". As we build up large collections of messages and photos over time, they can become a liability as well as an asset. For example, many people who have been on Facebook for a long time have photos from when they were younger that could be embarrassing. But people also really love keeping a record of their lives. And if all posts on Facebook and Instagram disappeared, people would lose access to a lot of valuable knowledge and experiences others have shared.

I believe there's an opportunity to set a new standard for private communication platforms – where content automatically expires or is archived over time. Stories already expire after 24 hours unless you archive them, and that gives people the comfort to share more naturally. This philosophy could be extended to all private content.

For example, messages could be deleted after a month or a year by default. This would reduce the risk of your messages resurfacing and embarrassing you later. Of course you'd have the ability to change the timeframe or turn off auto-deletion for your threads if you wanted. And we could also provide an option for you to set individual messages to expire after a few seconds or minutes if you wanted.

It also makes sense to limit the amount of time we store messaging metadata. We use this data to run our spam and safety systems, but we don't always need to keep it around for a long time. An important part of the solution is to collect less personal data in the first place, which is the way WhatsApp was built from the outset.

Interoperability

People want to be able to choose which service they use to communicate with people. However, today if you want to message people on Facebook you have to use Messenger, on Instagram you have to use Direct, and on WhatsApp you have to use WhatsApp. We want to give people a choice so they can reach their friends across these networks from whichever app they prefer.

We plan to start by making it possible for you to send messages to your contacts using any of our services, and then to extend that interoperability to SMS too. Of course, this would be opt-in and you will be able to keep your accounts separate if you'd like.

There are privacy and security advantages to interoperability. For example, many people use Messenger on Android to send and receive SMS texts. Those texts can't be end-to-end encrypted because the SMS protocol is not encrypted. With the ability to message across our services, however, you'd be able to send an encrypted message to someone's phone number in WhatsApp from Messenger.

This could also improve convenience in many experiences where people use Facebook or Instagram as their social network and WhatsApp as their preferred messaging service. For example, lots of people selling items on Marketplace list their phone number so people can message them about buying it. That's not ideal, because you're giving strangers your phone number. With interoperability, you'd be able to use WhatsApp to receive messages sent to your Facebook account without sharing your phone number – and the buyer wouldn't have to worry about whether you prefer to be messaged on one network or the other.

You can imagine many simple experiences like this – a person discovers a business on Instagram and easily transitions to their preferred messaging app for secure payments and customer support; another person wants to catch up with a friend and can send them a message that goes to their preferred app without having to think about where that person prefers to be reached; or you simply post a story from your day across both Facebook and Instagram and can get all the replies from your friends in one place.

You can already send and receive SMS texts through Messenger on Android today, and we'd like to extend this further in the future, perhaps including the new telecom RCS standard. However, there are several issues we'll need

to work through before this will be possible. First, Apple doesn't allow apps to interoperate with SMS on their devices, so we'd only be able to do this on Android. Second, we'd need to make sure interoperability doesn't compromise the expectation of encryption that people already have using WhatsApp. Finally, it would create safety and spam vulnerabilities in an encrypted system to let people send messages from unknown apps where our safety and security systems couldn't see the patterns of activity.

These are significant challenges and there are many questions here that require further consultation and discussion. But if we can implement this, we can give people more choice to use their preferred service to securely reach the people they want.

Secure Data Storage

People want to know their data is stored securely in places they trust. Looking at the future of the internet and privacy, I believe one of the most important decisions we'll make is where we'll build data centers and store people's sensitive data.

There's an important difference between providing a service in a country and storing people's data there. As we build our infrastructure around the world, we've chosen not to build data centers in countries that have a track record of violating human rights like privacy or freedom of expression. If we build data centers and store sensitive data in these countries, rather than just caching non-sensitive data, it could make it easier for those governments to take people's information.

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. 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.

Of course, the best way to protect the most sensitive data is not to store it at all, which is why WhatsApp doesn't store any encryption keys and we plan to do the same with our other services going forward.

But storing data in more countries also establishes a precedent that emboldens other governments to seek greater access to their citizen's data and therefore weakens privacy and security protections for people around the world. I think it's important for the future of the internet and privacy that our industry continues to hold firm against storing people's data in places where it won't be secure.

Next Steps

Over the next year and beyond, there are a lot more details and tradeoffs to work through related to each of these principles. A lot of this work is in the early stages, and we are committed to consulting with experts, advocates, industry partners, and governments – including law enforcement and regulators – around the world to get these decisions right.

At the same time, working through these principles is only the first step in building out a privacy-focused social platform. Beyond that, significant thought needs to go into all of the services we build on top of that foundation – from how people do payments and financial transactions, to the role of businesses and advertising, to how we can offer a platform for other private services.

But these initial questions are critical to get right. If we do this well, we can create platforms for private sharing that could be even more important to people than the platforms we've already built to help people share and connect more openly.

Doing this means taking positions on some of the most important issues facing the future of the Internet. As a society, we have an opportunity to set out where we stand, to decide how we value private communications, and who gets to decide how long and where data should be stored.

I believe we should be working towards a world where people can speak privately and live freely knowing that their information will only be seen by who they want to see it and won't all stick around forever. If we can help move the world in this direction, I will be proud of the difference we've made.

Mark Zuckerberg is cofounder/CEO of Facebook, Menlo Park, CA.

This post was reproduced in its entirety from the original that Facebook CEO Mark Zuckerberg first ran March 6, 2019 on his Facebook page.

© 2020 Napean LLC. All rights reserved.

Luxury Daily is published each business day. Thank you for reading us. Your feedback is welcome.