PRIVACY OR FAIR COMPETITION: WHAT ARE APPLE'S IOS 18 INTENTIONS?

More data control for consumers should be good. But is Apple intentionally advantaging its own apps, thereby hurting competition and consumers? And should consumers be told when data choices will diminish their cyberprotection?

Data Catalyst Institute, September 2024

Summary

In mid-September 2024, Apple will release the next generation of iPhone software, iOS 18, for hundreds of millions of users. Apple says changes in iOS 18 will put "privacy at the core," which advocates and policymakers generally consider good for consumers. However, in this instance, how Apple implements giving consumers more control over their data may have anti-competitive and cybersecurity impacts that actually harm consumers.

Historically, iOS has offered consumers a simple, binary choice when new third-party apps are downloaded: share contacts or don't share contacts. However, with iOS 18, Apple's "share contacts" process will include more privacy options that embed subtle encouragement to reduce sharing. The impact of the additional choices is definitely that users get more control. Still, there is an additional impact that effectively promotes Apple-owned apps instead of third-party competitors that rely heavily on Contacts, e.g., for peer-to-peer communications, cybersecurity, and other features. This subtle self-preferencing highlights an important tradeoff between fair competition and consumer privacy, both of which have been top-of-mind for several years amongst policymakers in Washington, DC, state capitals, and globally.

Additionally, the new option to share only some Contacts with messaging apps opens the door to more spam, phishing, and hacking. This is also something that consumer advocates should be attentive to.

Analysis

Apple will release iOS 18, the latest version of its popular iPhone software, in mid-September 2024. Hundreds of millions of consumers use iOS 18 daily, and thus, changes to operating systems are significant for a wide range of consumers. As reported in the technology press, many iOS 18 changes offer clear benefits to iPhone users. These include upgraded photo and email organization features and AI-powered writing and transcription tools. The company says the changes will enhance iPhone users' experience, simplify everyday tasks, and put "privacy at the core." It is this last point that we examine here.

Currently, when iPhone users download third-party payment, messaging, and social apps with messaging functionality (e.g., Venmo, WhatsApp, and Roblox), the apps request access to users' contacts because contacts are critical to their functionality. iOS then confirms that users wish to allow contacts. If users agree, Apple will grant them access to the new apps. However, with "privacy at the core" in iOS 18, Apple will ask users a new, additional question: whether they want to share all their contacts or select only a few. "Share select contacts" will be presented as the first option, placed higher on the consumer's screen than the "Share all contacts" option. This enhanced data privacy feature - the option and encouragement to share only some contacts - is likely to harm third-party apps and promote Apple apps in two significant ways.

- **Inconvenient installation.** Requiring iPhone users to answer two questions and manually select contacts makes installing third-party apps less convenient. This will substantially reduce the number of these apps installed and divert consumers back to Apple's owned and default apps, e.g., iMessage and Apple Cash.

- **Increased cyber vulnerabilities.** Comprehensive contact data is essential for maintaining messaging integrity and preventing scams and spam within payment and messaging apps. Limiting access through a "select contacts" option will significantly undermine the safety and security of third-party apps, exposing consumers and their contacts to greater risk. As vulnerabilities in these apps become more apparent, users are likely to only use Apple's proprietary apps.

TABLE 1: PROMINENT THIRD-PARTY APPS HARMED BY IOS 18 PRIVACY CHANGES

APP	PARENT CO	CATEGORY	APPLE EQUIV.	POTENTIAL HARM
CashApp	Block	Fintech	Wallet	Harder to send/receive money from contacts
ChatGPT	OpenAI	Comms	Siri	Harder to place calls or send messages to contacts via AI
Gemini	Google	Comms	Siri	Harder to place calls or send messages to contacts via AI
Google Photos	Google	Leisure	Photos	Harder to use the “Shared with you” feature for Google users who are also in phone contacts
Outlook	Microsoft	Comms	Mail	Harder to use emails of current contacts
Roblox	Roblox Corp	Leisure	Messages, Phone, FaceTime	Harder to start calls or send messages and harder to screen inbound calls and messages
Signal	Signal Technology Foundation	Messaging	Messages, Phone, FaceTime	Harder to start calls or send messages and harder to screen inbound calls and messages
Snapchat	Snap	Messaging	Messages, Phone, FaceTime	Harder to send messages
Venmo	Paypal	Fintech	Wallet	Harder to send/receive money from contacts
WhatsApp	Meta	Messaging	Messages, Phone, FaceTime	Harder to start calls or send messages and harder to screen inbound calls and messages

Discussion

Our analysis reveals a hidden tension between two major technology policy and regulation trends from Washington, D.C., state capitals, the EU, and globally. One is the push for enhanced data privacy, security, and user control. The other is the enhanced scrutiny of large tech platforms' competition and self-preferencing practices in advertising, e-commerce, social media, and other areas.

However well-intentioned, when powerful platforms swing the regulatory pendulum, even in favor of data privacy, it can distort markets and create or incentivize self-preferencing. In this instance, Apple Messages, FaceTime, Photos, Wallet, and Siri will be self-preferenced compared to third-party competitors such as Signal, Google Photos, Venmo, ChatGPT, and many others.

Additionally, there is a cyber-vulnerability dimension to this equation. Suppose messaging and payments apps don't have access to a person's entire contacts list. In that case, they cannot monitor for spam and validate trusted messages by determining if a message is coming from an existing contact. (Apple uses contacts this way for its own apps – for example when you get an iPhone text from an unknown sender not in your contacts, you get a "Report Junk" prompt.) Similarly, there is a vulnerability if a message sender impersonates someone a user knows, but the app cannot verify that by accessing contacts. As spammers and cybercriminals learn that third-party apps don't have access to full contact data, they will undoubtedly focus their targeting efforts on non-Apple apps such as Signal, WhatsApp, and Venmo.

Cybersecurity and competition are too important, and the iOS platform is too big to ignore these large platform concerns. Regulators, academics, and consumer groups must consider the implications and motivations behind Apple's so-called privacy improvement. They should particularly consider them from a consumer welfare perspective, asking questions such as:

- If privacy is indeed Apple's goal, why not offer users the same "share all contacts vs. share select contacts" choice for Apple's contact-dependent apps?

- Assume the primary goals of the iOS 18 upgrades include improved user experience and easier completion of everyday tasks. Why make it more difficult for users to download apps that enable everyday activities such as transferring money and messaging friends and family?