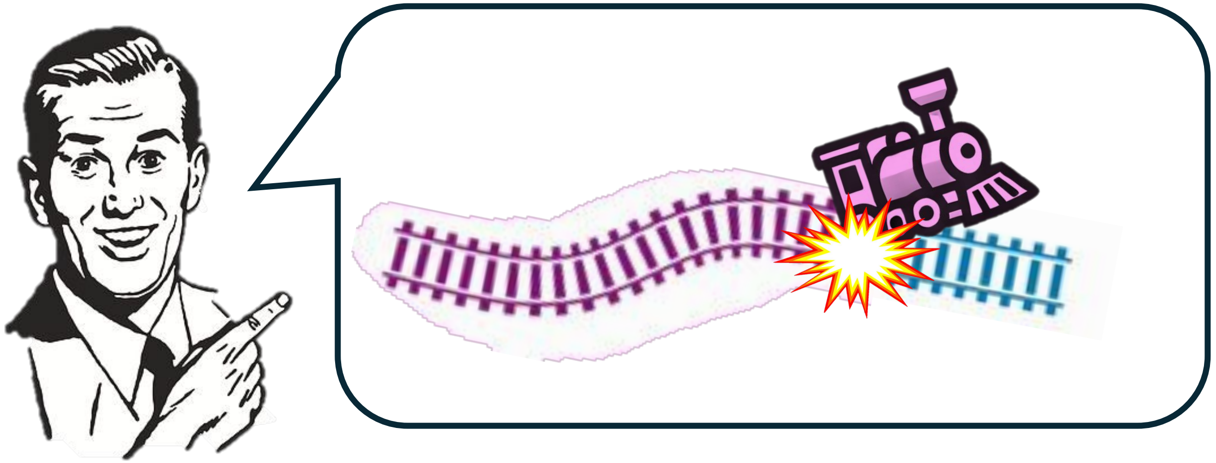
“Interoperability vs Security” Arguments: An Analytical Framework

With Elettra Bietti and Sunoo Park

What is the problem?

- There are regulatory efforts to get companies to **interoperate**
- Those companies don't want to
- So they use **security arguments** to push back



"Although we hope that alternative app marketplaces will meaningfully invest in protecting user security, privacy, and safety, we cannot guarantee it." – Apple 2024

"Data-hungry companies across the globe may weaponize interoperability" – Apple 2024

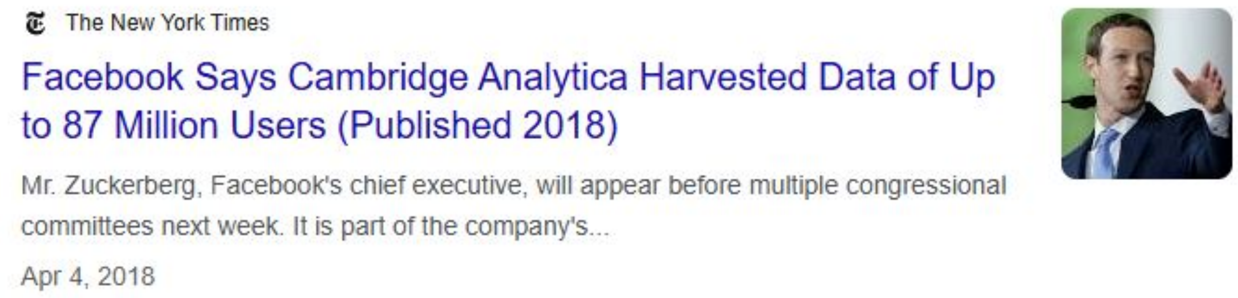
"The new options we're introducing to comply with the DMA necessarily mean we will not be able to protect users in the same way" – Apple 2024

"If Apple is forced to allow access to sensitive technologies that it has no ability to protect, the security risks would be substantial and virtually impossible to mitigate." – Apple 2024

"[W]e are now seeing concrete examples of how a new approach to interoperability in the EU would put users at risk." – Apple 2024

"[t]he [interoperation] requirement … effectively requir[es] Google to endorse stores that might be full of harmful content" – Google 2025

Security and interoperability aren’t so simple



The New York Times

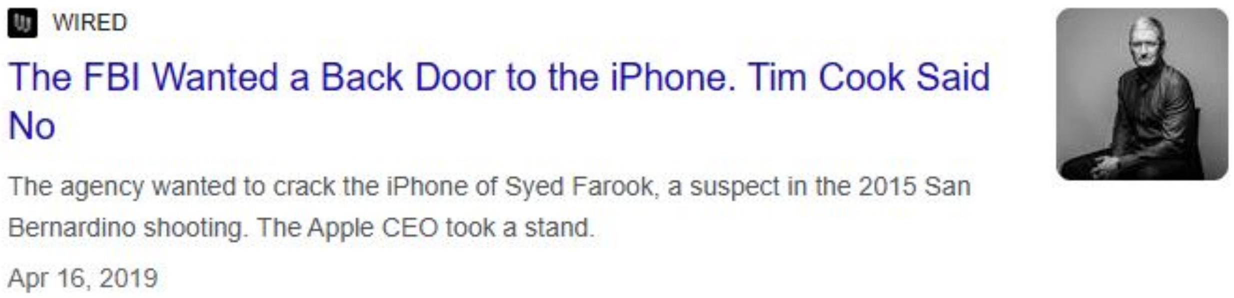
Facebook Says Cambridge Analytica Harvested Data of Up to 87 Million Users (Published 2018)

Mr. Zuckerberg, Facebook's chief executive, will appear before multiple congressional committees next week. It is part of the company's...

Apr 4, 2018

Facebook made an interoperability feature that allowed third parties access to user friends’ information. Cambridge Analytica used this feature to access the data of millions of users.

Apple refused to create a back door to the iPhone after the San Bernardino shooting because this would undermine the security of the operating system. The security community generally agrees with Apple’s decision.



WIRED

The FBI Wanted a Back Door to the iPhone. Tim Cook Said No

The agency wanted to crack the iPhone of Syed Farook, a suspect in the 2015 San Bernardino shooting. The Apple CEO took a stand.

Apr 16, 2019

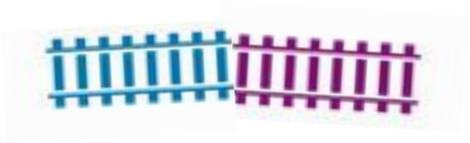
Our Contribution

- How to spot a security boogeyman:
  - Look at the **structure of interoperation**
  - What are the **security vs interoperability** arguments?
  - How do these arguments interact with both the **economic** and **technical** realities?

Structure of Interoperation

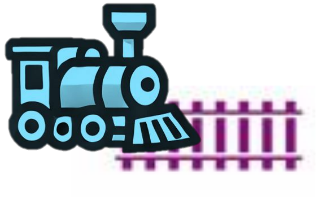
Horizontal

- Between competitors with similar, competing products
- Economic substitutes



Vertical

- Between platforms and the products that run on them
- Economic complements



This structure largely mirrors the economic relationships

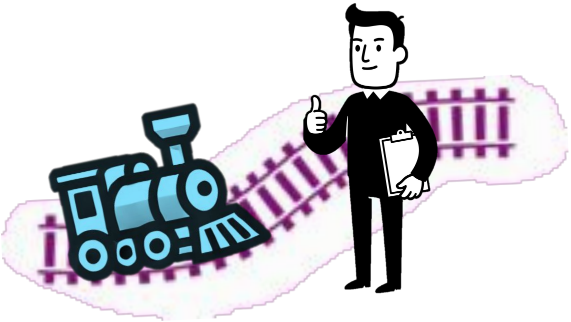
Security vs Interoperability Arguments

Engineering Concerns

- Secure interoperability needs to be **built** and this is hard if not impossible

Vetting Concerns

- Changing security **policies** that stand in the way of interoperability would be risky



And sometimes both!

Hybrid Concerns

- Arise in cases where a third-party product would run on an incumbent company’s platform (**vertical interoperation**)
- Would require both **engineering** (opening up unavailable functionality) and **vetting**
- We see these concerns when the incumbent company is **self-preferencing** its own complementary products

Examples

Engineering Concern

iMessage

WhatsApp

Messenger

Vetting Concern

Buy with In-App Purchase

Google Play

App Store

WebKit

EPIC GAMES STORE

Hybrid Concern

Pay

fitbit

AirDrop

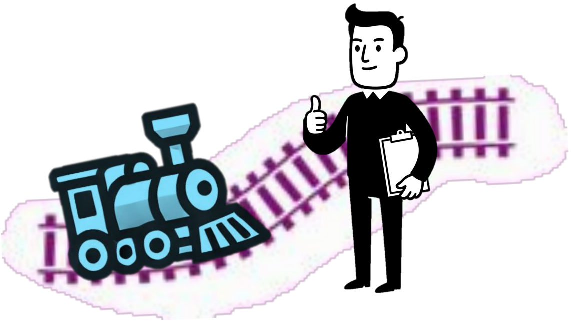
Security Engineering Concerns

- Secure interoperation is going to require substantial changes or additions to the current system
- This is generally difficult to do securely and there is substantial security literature detailing these difficulties

"While [Meta has] built a secure solution for interop that uses the Signal Protocol encryption to protect messages in transit, without ownership of both clients (endpoints) we cannot guarantee what a third-party provider does with sent or received messages, and we therefore cannot make the same promise." – Meta 2024

Vetting Concerns

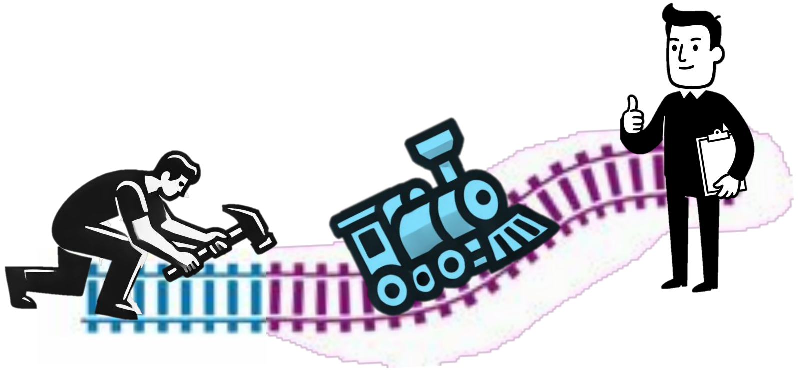
- Platform owners can completely block third-party developers from their users if the third-party products go against policies
- Platforms are incentivized to extract fees, not block access entirely
- Vetting can still take place under changed fee and distribution regimes



"[t]he [interoperation] requirement … effectively requir[es] Google to endorse stores that might be full of harmful content, ranging from malware that can scam or extort users to pornography and hate speech."
– Google 2025

Hybrid Concerns

- Platforms can use both types of concerns
- Generally the incentive is for platforms not to facilitate interoperation at all and defend existing self-preferencing
- But this is more sensitive technology



"If Apple is forced to allow access to sensitive technologies that it has no ability to protect, the security risks would be substantial and virtually impossible to mitigate." – Apple 2024

Conclusion

Engineering concerns – these are hard engineering problems, listen to experts and standards bodies

Vetting concerns – platforms are incentivized to keep third parties in their walled gardens to extract fees and monitor security

Hybrid concerns – platforms are incentivized to prevent the entry of third-party developers entirely