

“Security vs. Interoperability” Arguments: An Analytical Framework

Daji Landis
New York University

Elettra Bietti
Northeastern University

Sunoo Park
New York University

Abstract—Concerns about big tech’s monopoly power have featured prominently in recent media and policy discourse, as regulators across the EU, the US, and beyond have ramped up efforts to promote healthier market competition. One favored approach is to require certain kinds of *interoperation* between platforms, to mitigate the current concentration of power in the biggest companies. Unsurprisingly, interoperability initiatives have generally been met with resistance by big tech companies. Perhaps more surprisingly, a significant part of that pushback has been in the name of *security*—that is, arguing against interoperation on the basis that it will undermine security.

We conduct a systematic examination of “security vs. interoperability” (SvI) discourse in the context of EU antitrust proceedings. Our resulting contributions are three-fold. First, we propose a *taxonomy* of SvI concerns in three categories: engineering, vetting, and hybrid. Second, we present an *analytical framework* for assessing real-world SvI concerns, and illustrate its utility by analyzing several *case studies* spanning our three taxonomy categories. Third, we undertake a *comparative analysis* that highlights key considerations around the interplay of economic incentives, market power, and security across our diverse case study contexts, identifying common patterns in each taxonomy category. Our contributions provide valuable analytical tools for experts and non-experts alike to critically assess SvI discourse in today’s fast-paced regulatory landscape.

1. Introduction

Billions of users entrust vast amounts of personal data to their devices and to services that are controlled by a small number of very large companies. These companies have huge discretion over whom to share this data with, and how to secure these vast data flows—in messaging, digital payments, tap-and-go technology, and more.

Recent concerns around concentration of power in big tech have led to calls and legal mandates for platforms to support increased interoperation [24], [48], [50], [54], [80]. The idea is that interoperation would open the market to more smaller players, promoting healthier competition, especially where a single market actor holds expansive control over a software and/or hardware ecosystem. Large tech platforms, on the other hand, have every incentive to resist moves to open up their systems to interoperate.

In this context, companies seeking to resist interoperability mandates are increasingly arguing that the security of their systems requires keeping them closed and limiting competition. They describe their systems’ security as a key business proposition, and a key reason consumers are attracted to their business models.

These kinds of statements tend to appear in public-facing communications and sometimes legal or regulatory

filings. As such, they typically remain high level, and do not get into technical detail on the precise nature of the claimed tensions between security and interoperation. By way of illustration, Google recently argued against mandated interoperation with alternative app stores in a case in front of the US Supreme Court:

“[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.”¹

Such “security vs. interoperability” arguments are often framed as technical arguments about incurring unacceptable security risks—an area outside the usual expertise of courts and policymakers, and squarely within that of the tech companies subject to regulation.² Perhaps the most prominent past instance where companies made technical arguments about incurring unacceptable security risks was in resisting government efforts to weaken encryption [36]—in that context, the companies were widely seen as the champions of the public interest.³ Arguments about the security risks of interoperation may carry particular weight—for policymakers, regulators, and the general public—when raised by the same companies, which are already responsible for vast amounts of sensitive data that could be imperiled by ill-advised regulation and have established reputations for security and privacy.

Although companies should be able to put forward the best case for their own interests in such regulatory contexts, this trend is concerning if and when seemingly technical arguments are treated with more deference than business or policy arguments, as more objective or factual, or as matters on which courts and regulators should defer to companies’ technological expertise.

The defining characteristic of “security vs. interoperability” arguments is the potential for them to instrumentalize “security” into a cause for deference that is convenient for business ends. Consider the quote above—Google is right: alternative app stores may contain lots of malware. *But does this argument mean that regulators should drop their antitrust efforts because of the grave security harm that Google argues will result?* That does not follow directly. The security community might say that is a question of antitrust law or policy and beyond our domain—but the answer to that antitrust question hinges on a security question beyond antitrust experts’ domain.

1. Application for Partial Stay of Permanent Injunction Pending Disposition of Petition for a Writ of Certiorari, *Google LLC v. Epic Games, Inc.*, No. 25A (U.S. Sept. 24, 2025)

2. Not only because of technological expertise in general, but also due to companies’ detailed knowledge of how their own systems work.

3. These security-critical arguments may well have served the companies’ business interests as well.

The “security vs. interoperability” narrative is an inherently interdisciplinary one, about acceptable tradeoffs in integrating technical security goals with other policy goals. The availability of alternative app stores raises security risks, which may be balanced against other benefits, such as a more competitive marketplace. Focusing on only technical aspects or only economic or regulatory aspects yields an inherently incomplete picture, and policymaking based on such a view could lead to missteps in the important and fast-moving area of big tech and antitrust. Thus, it is critical for the security community to engage with “security vs. interoperability” questions not by opining on isolated technical questions but by embracing the broader economic and policy context in which these arguments appear—especially when industry interests may not align with highlighting this broader scope. Our engagement is essential to complement lawyers, regulators, and policymakers in this impactful space, to clarify and mitigate potential security harms of antitrust initiatives.

This paper provides a blueprint for doing just that, based on a systematic review of relevant cases in the EU. We present a *taxonomy* that divides “security vs. interoperability” tensions into three key categories: engineering, vetting, and hybrid. The hybrid case combines aspects of both engineering and vetting issues, and exhibits more complex dynamics than either alone due to their interplay. Our *analytical framework*, illustrated via a series of detailed *case studies* from the EU, captures the key economic considerations relevant to the regulatory context in which the “security vs. interoperability” discourse is rapidly unfolding.⁴ Our framework is designed to be usable without knowledge of antitrust law or economics, and captures key aspects and patterns across all of the real-world cases we systematically examine. For each case study, we provide detailed analysis of the security, interoperability, and incentives considerations. These case study analyses illustrate our approach’s utility in disentangling where security and interoperability are and are not in tension, where securing interoperable systems presents novel engineering challenges, and where “security arguments” against interoperability may be a distraction from the real issue: fair competition. Finally, our *comparative analysis* identifies common patterns in the interplay of incentives, market power, and security in each taxonomy category.

Broader context and motivation. The use and misuse of security arguments is an issue of natural interest to the security community. In the present context, the broader implications lie as much in security outcomes as in competition policy outcomes, and the timeliness and potential breadth of impact of the “security vs. interoperability” issue arises more from today’s competition policy context than from the field of security.

The concentration of economic and political power in the hands of a few technology companies, alongside the novelty, complexity, and opacity of modern technology, has contributed to a climate in which companies may strategically deploy (seemingly) technical arguments to further their political and economic power and avoid

regulation. Recent legal scholarship has highlighted companies’ strategic use of privacy, content moderation, and security arguments to further economic and policy interests [33], [40], [60], [68], [70]. Van Loo [60] discusses how companies use privacy inconsistently as a pretext to further business aims, including to limit competitors’ access to data, while engaging widely in data selling and sharing when beneficial for business.

This paper focuses on companies’ security-related discussion in the context of antitrust investigations in the European Union that involve mandated interoperability. When companies raise security arguments in this context, in general, the criticality and nuances of the security issue cannot be expected to be transparent to lawyers, courts and policymakers, or to other public stakeholders.

Companies seeking to defend themselves from competition claims may strategically bring in security experts. Those seeking to impose competition obligations will, in turn, bring their own security experts. In the *Epic v. Apple* case, companies’ experts have asserted that a system might suffer serious security risks or degradation if the company is forced to comply with interoperability obligations, and the opposing experts have argued that this is not true [63].⁵

We believe our systematic analysis of “security vs. interoperability” discourse can help the security and policy communities better analyze and conceptualize “security vs. interoperability” tensions (and the lack thereof), leading to better policy decisions that will shape the future of technology markets and ecosystems.

Those policy decisions may go either way, depending on the context—we are not arguing for particular outcomes. We caution against “security vs. interoperability” arguments’ potential use as a pretext to further business aims; equally, we caution against underestimating the real security challenges in building interoperable systems. These two cautions go hand in hand: distinguishing one from the other is the crux of the difficulty for judges and policymakers, when business interests often favor companies making both these kinds of arguments and making them hard to distinguish from one another.

Other related work. That security engineering requires consideration of contextual sociotechnical factors is hardly a new observation [3]. The security economics literature has long highlighted and studied the idea that “security failure is caused by bad incentives at least as often as by bad design” [2], [4]. Much of security economics considers how incentives influence security outcomes. Our inquiry takes a different angle, in a similar spirit: we ask how security arguments can be leveraged to serve other economic goals.

Digital competition policy and antitrust enforcement have been responding to digital markets trends long before the recent wave of interest in big tech and antitrust. Microsoft’s bundling of Internet Explorer with Windows was the subject of a landmark 1998 antitrust case.⁶ Net neutrality regulations, which required internet service providers not to give preferred treatment to certain types of content or traffic for economic reasons,

4. The EU has focused heavily on Apple in its recent interoperation-related antitrust efforts. As a result, our case studies mostly involve Apple, as further discussed in Section 2 (Note 3).

5. The “battle of the experts” problem is a much broader problem with expert witnesses in legal systems [45].

6. *United States v. Microsoft Corporation*, 253 F.3d 34 (D.C. Cir. 2001).

have been at the heart of political controversies since the 1990s [42], [51], [77], [78], [82]–[84]. The “security vs. interoperability” narrative, our focus in this paper, is a more recent development that very little prior work has considered. Since the European Union’s Digital Markets Act (DMA), a promising initial literature has begun to examine the complexities of securely interoperating end-to-end encrypted messaging [25], [55].

Summary of contributions. We critically examine “security vs. interoperability” (SvI) discourse related to antitrust proceedings in the European Union (EU). Our four key contributions are as follows.

- 1) We conduct a **systematic review of EU competition cases** involving interoperability mandates for digital technology, which feature SvI considerations (§2).
- 2) We propose a three-part **taxonomy** of SvI concerns, and explain the taxonomy’s relationship to the economic concepts of *vertical* and *horizontal* interoperability (§3).
- 3) We introduce an **analytical framework** centered around four critical questions, and apply it to **six case studies** across diverse contexts featuring SvI concerns: messaging, app sideloading, app stores, browser engines, NFC, and physical device interoperation (§4).
- 4) We offer a **comparative analysis** of these case studies through the lens of our framework, illuminating *key patterns in the interplay of economic incentives, market power, and security* in each taxonomy category (§§4–5).

2. Our Methodology

We systematically reviewed cases where security comes up in the context of mandated interoperability in antitrust proceedings. We focus on EU cases, as there has been extensive and well documented surge of relevant antitrust enforcement activity in the EU in the past few years. Similar issues have arisen in US antitrust proceedings; we will note examples of prominent parallel US cases.

We first collected all cases in which there have been interoperability mandates related to digital technology, in the EU Commission’s competition case database [37] (henceforth, ‘EU Database’). We then searched for discussions about security in the context of our selected cases. The resulting collection of discourse—from legal and regulatory proceedings, press releases and press coverage, developer-facing documentation, and consumer-facing information—forms the basis for our systematization and analysis.

The rest of this section details: (1) how we selected our cases; (2) high-level results of our screening process; (3) how we tagged these cases with relevant technologies; and (4) how we identified relevant security issues.

What we mean by ‘interoperation’. We use *interoperation* to refer broadly to practices in which products or services produced by one company (e.g., smartphones) support or facilitate user engagement with products or services developed by a third-party (e.g., independent apps). For our purposes, interoperation comprises both *technical interoperability* (e.g., what are the technical requirements for an app to run on a given platform?) and *interoperation policy* (e.g., which technically interoperable apps does a platform permit as a matter of policy?).

2.1. Search Methodology

The EU Database features five categories of ‘policy areas,’ of which only three are within our scope: ‘Antitrust & Cartels,’ ‘Digital Markets Act,’ and ‘Merger.’⁷

In our initial search, we searched all cases in either the ‘Antitrust & Cartels’ or the ‘Digital Markets Act’ policy area. In a follow-up search, we covered ‘Mergers’ with narrowed search criteria (including limited economic activities), a refinement we discuss below. In both the initial and the follow-up search, we used the search terms ‘interoperate interoperability interoperation,’ which the EU Database search engine interprets as a disjunction.

Given the specific definition of interoperation we seek to capture, we conducted a preliminary search of DMA cases in the EU Database to check whether our search terms were used with the meaning we intended to capture. We found that the search terms were used in reference to both *technical interoperability* and *interoperation policy*, as defined above. We also tried other similar terms such as ‘compatible’ or ‘integrated’ and found these did not capture any cases we deemed relevant that were not in our original search.

From the results of our initial and follow-up searches, we manually screened for cases satisfying the following additional criteria: (1) the case concerned interoperation of digital technologies (not, e.g., trains), and (2) the case related to interoperation mandated by antitrust authorities. Section 2.2 offers more detail on the screening process.

Based on our initial search of Antitrust and DMA cases, we manually identified which classifications of economic activities⁸ included relevant digital technologies. We used these classifications⁹ to filter and improve efficiency in our follow-up search of Merger cases.¹⁰

2.2. Screening for Relevant Cases

Our screening process consisted of two main phases: an initial screening based on a quick read, and a second phase where a more thorough reading was necessary.

Phase 1 (P1). We filtered out any cases that were dismissed or that were just DMA ‘gatekeeper’ designations¹¹ as these cannot give rise directly to interoperability mandates. We moreover filtered out cases that were quickly identifiable as out of scope, for one of the following reasons. First, many cases used the term interoperability only once, in a common definition of ‘Standards’—we discarded cases where this was the only mention of the term. Second, some cases mentioned interoperability a few times only as an existing product feature or part of the

7. The other categories are ‘Foreign Subsidies’ and ‘State Aid.’

8. These are classifications of industry made by the EU [39]

9. We included the following codes: NACE Rev 2 (2008): C.26.1, C.26.2, C.26.3, C.26.4, C.26.51, J.61.2, J.61.9, J.62, J.63, K.64.99; NACE Rev 2.1 (2025): C.26.1, C.26.2, C.26.3, C.26.4, C.26.51, K, L.64.9.

10. We first eliminated codes that were unlikely to be about digital technology (e.g., C.10.52 - Manufacture of ice cream), and included any codes directly pertaining to digital technology. For the remaining codes (e.g., regarding finance), we omitted codes associated only with one or more non-relevant cases in the initial search, and kept all others.

11. The term gatekeeper as defined in the DMA Article 3 refers to entrenched incumbent companies that provide platforms that are important for third parties to be able to reach end users.

regulatory context; these cases did not involve mandates in their mentions of interoperability, so we discarded them. Third, sometimes multiple cases appear in the same document; we discarded cases in the same document as a mention of interoperability, that do not themselves mention the term. Phase 1 eliminated the majority of irrelevant cases (see Table 1).

Phase 2 (P2). All cases that remained required a more thorough reading to establish whether they were within our scoping criteria. We removed a number of cases that discussed interoperability as a product feature or important context in greater depth than was readily apparent, but did not mention interoperability *mandates*. We also removed one case that was not about digital technology. The resulting 14 cases are listed in Table 4 (Appendix).

Policy area	Initial count	Removed in P1	Removed in P2	Kept
Antitrust	28	22	4	2
DMA	17	13	0	4
Merger	66	45	13	8

TABLE 1. NUMBER OF CASES BY POLICY AREA

Note 1 (Merger case selection). Among the Merger cases, many discussed potential interoperability issues but did not ultimately have an interoperability mandate. Generally this was because the Commission decided that the potential benefit to the merged entity of degrading interoperability was either not incentive compatible (i.e., not a good business decision) or not feasible. In a few cases the degrading was not deemed to be significant enough to greatly impact the market. In those cases we kept, there was some commitment regarding interoperation that was required for the merger.

2.3. Identifying Relevant Technologies

With these fourteen cases in hand, we next identified the technology or technologies that were the subject of (potential) interoperability mandates. The cases often discussed many products and not all were necessarily related to interoperability mandates. Some cases discussed multiple distinct technologies subject to interoperability mandates. Some distinct cases discussed the same type of technology. We define the *relevant technologies*, within a case context, to be the technologies subject to interoperability mandates. Table 4 (Appendix) lists relevant technologies for each case.

In some cases, we looked up mentions within the selected cases, of apparently similar cases about similar technologies. This led to detailed review of one EU case beyond the 14 selected (on WhatsApp and Messenger).¹²

2.4. Identifying SvI Considerations

Next, we collected discussion about the security implications of interoperability mandates—that is, SvI considerations—in each of our selected cases, across three sources: (1) the relevant company’s public-facing statements about the case, (2) mentions of security in relevant

legal and regulatory proceedings, and (3) developer-facing information regarding the technical details of the relevant interoperation. By SvI considerations, we mean any actual, potential, perceived, or claimed tensions between security goals and mandated interoperation.

We collected such discussion by searching the press releases and developer documentation of the companies involved during the relevant time period, as well as Google searches for the company name and relevant technology alongside various combinations of the search terms ‘merger,’ ‘antitrust,’ ‘DMA,’ ‘EU,’ ‘Commission,’ ‘security,’ and ‘privacy.’ Note that this process might not have captured all company communications, especially for older cases, as search interfaces and archives for press releases and developer documentation were variable.¹³ We found company publications or news articles with official statements about every case, although many did not mention security or mandated interoperability.

For mergers in particular, there was generally no discussion of the details of the commitments in public-facing venues. The only exception to this was the Google/Fitbit merger. As mergers are voluntary, they tend to involve situations in which companies are incentivized to make the merger appear favorable to shareholders and customers. In contrast to other antitrust proceedings, therefore, companies may be disincentivized from publicly suggesting that a merger will be disadvantageous to their security.¹⁴

Not every selected case involved an SvI concern. For some cases, we did not find any mentions of security at all: for example, the Cisco/Tandberg merger did not discuss the security of the underlying technology at all.¹⁵

Note 2 (Interoperability without security). For those cases where we found no relevant security issues, we found a natural sub-categorization emerged, according to the type of interoperability mandate. All such cases we examined either required (1) that interoperability not be degraded in future, (2) that information related to interoperability be disclosed (but no further facilitation of interoperability was required), or (3) both. Table 4 (Appendix) marks such cases as having ‘No’ SvI concern, followed by a sub-category (‘Degrade,’ ‘Disclose,’ or ‘Both’).

Note 3 (Prevalence of Apple cases). The EU has initiated many proceedings against Apple in particular. In the cases pertaining to app stores (Section 4.2), the EU has focused on Apple alone. In the US, cases brought by Epic Games, maker of Fortnite, against *both* Apple and Google, alleged similar antitrust behavior from both companies.¹⁶ Our case studies focus mostly on Apple, mirroring the cases captured in our EU-focused methodology. We believe the analogous behavior on the part of Google is sufficiently similar that our analysis is likely to generalize.

13. Our oldest case was decided in 2004, and the oldest relevant press release we were able to find is now only available on the Internet Archive.

14. Companies may make security arguments to the Commission that are not public [56], to which we did not have access.

15. Some of the mergers had surrounding discussion that said the merger and resulting interoperability (independent of any mandates) would *improve* consumer security as in the Intel/McAfee case.

16. See *Epic Games, Inc. v. Google LLC*, Nos. 24-6256, 24-6274, 2025 WL 4720491 (9th Cir. July 31, 2025), settled (Nov. 5, 2025) and *Epic Games, Inc. v. Apple Inc.*, 67 F.4th 946 (9th Cir. 2023), cert. denied, 144 S. Ct. 681 (2024).

12. DMA.100024 Meta – number-independent interpersonal communications services

2.5. Systematization and Analysis

Our detailed review of these collected cases and materials, found three clear patterns—or categories—in the nature of the security arguments and the nature of changes needed to comply with the relevant interoperability mandate that form the basis for our taxonomy of SvI concerns (§3). The interplay of security and economic considerations that we observed repeatedly in the cases and materials formed the basis for our analysis questions (§4). We chose one to three case studies to feature for each taxonomy category, aiming to capture diverse and well-documented issues (§4).

3. Our Taxonomy

We now introduce our three-part taxonomy, which distinguishes two broad types of “security vs. interoperability” arguments as raising either security *engineering* concerns or security *vetting* concerns, alongside a third *hybrid* category that raises concerns incorporating aspects of both other categories. Table 2 provides an overview. Our taxonomy clarifies the different types of security concerns that may arise in response to the prospect of introducing interoperation between products or systems which did not previously interoperate.

The technical, economic, and policy contexts in which these concerns are raised is critical to our taxonomy and subsequent analysis (§§4–5). In particular, the status quo of how the systems in question work *before* interoperation is introduced, the nature of the technical security guarantees the systems already provide, and the security policies and tradeoffs already in place, are essential considerations.

Security Engineering Concerns. When considering introducing interoperation to systems that are not technically interoperable, preserving security alongside interoperation may require that some aspect of the company’s product or architecture be non-trivially changed. How to change systems to preserve the security guarantees currently offered, while also supporting interoperation, may or may not be clear based on existing techniques.

In such contexts, companies may raise concerns about the costs and engineering challenges that would be required to preserve security while supporting interoperability. We call these *security engineering concerns*.

Template of a Security Engineering Concern

- 1) Interoperating would require a building new technical mechanism or architecture for our system to interface with other systems.
- 2) Our system has existing technical security guarantees. Designing a new architecture to preserve these guarantees is an engineering task that is costly in time, effort, and coordination with others—and may require innovation, so success is not certain.
- 3) Therefore, interoperating secure systems is more costly than interoperating systems in general, and if we don’t get the engineering right, the security of billions of users could be undermined.

Security engineering concerns tend to arise when there are two (or more) parties trying to interoperate similar services while maintaining the technical security guarantees of their existing system designs. Historically, in

such situations, all parties involved need to develop, agree on, and implement compatible protocols or systems, so the security engineering concern is shared among all the parties seeking to interoperate. In contrast, the recent EU interoperation mandates allow ‘gatekeepers’¹⁷ to decide many aspects of the terms on which others may interoperate with them. Messaging services provide a clear example of a security engineering concern (see Section 4.1).

Note 4 (Securely engineering interoperation is hard).

Coordinating between systems managed by different parties is inherently complex. Security engineering in such decentralized or federated contexts can present novel challenges not present in the context of centralized systems—as well known in the security literature through a long history of examples such as PGP [46], [81], TLS [53], DNSSEC [57], MLS [1], and blockchains [27], [66]. Each of these required a negotiated standard and widely distributed implementation and maintenance. Related challenges include consensus building and communication as well as consistent implementation and enforcement of security standards over time. It seems possible that the EU approach—of assigning broad authority to ‘gatekeeper’ entities to set the terms of interoperating with their systems—may alleviate some of these complications, especially as regards consensus building. That said, engineering interoperation with powerful ‘gatekeepers’ still raises complex technical challenges and open questions (see our case study on messaging in Section 4.1).

Security Vetting Concerns. Security vetting concerns arise in contexts where there is already some kind of interoperation supported by a system’s technical architecture. Many devices and platforms support an ecosystem of apps, software, and connected devices that are integral parts of their functionality, but that are developed by third parties. Examples include platforms, browsers, or operating systems on which third-party software can run, and platforms that offer API access to third-party developers.

Given such an architecture, there remains the question of which third parties a platform is willing to interoperate with. Downloads and other connections can open a vector of attack for malware, spyware, and other undesirable outcomes for both the user and the device. Companies may vet and control which apps, systems, or software are permitted to interact with their devices with a view to preventing or mitigating such undesirable security outcomes—although these decisions might be motivated by other goals too.

Template of a Security Vetting Concern

- 1) Interoperating would mean our users and systems interacting with third parties and third-party software.
- 2) Third parties and third-party software may make different decisions about security than us. We cannot guarantee that third-party software would adhere to the same standards as software we have developed or carefully examined ourselves.
- 3) Therefore, allowing third-party software on our platform could undermine billions of users’ security.

In such contexts, when asked to support greater interoperation, companies may raise concerns that third-party

17. See footnote 11.

Type of concern	Starting point	Relevant security status quo	Mitigation
<i>Engineering</i>	No <i>technical</i> interoperability	Technical security guarantees of existing system design	Build something new (if possible; may require <i>technical innovation</i>)
<i>Vetting</i>	No/onerous/costly interoperation as a matter of <i>policy</i>	Security protections of existing interoperation policy	Vet third parties and products as a condition of interoperation
<i>Hybrid</i>	Integrated in-house interoperation, with no support for third parties	Security of in-house products and in-house product integration	Build technical support for third-party products and vet them

TABLE 2. OVERVIEW OF OUR TAXONOMY

software that interoperates with their systems may not be as secure as their own systems, and thus undermines the security of their users and/or systems. We call these *security vetting concerns*.

Vetting third parties can be an important way to protect users, but also concentrates power and discretion of incumbent companies over ecosystems they control. Companies in this position can use their role as security guarantor to charge developers for access or prevent competitors from reaching the market. Platforms’ interoperation policy choices thus require striking a tradeoff between security, interoperation, and other business considerations.

Due to the discretionary tradeoffs involved, arguments that security considerations *necessitate* a particular form of vetting or security measures generally cannot be substantiated by purely technical reasoning. Rather, they must refer to existing interoperation policies and the discretionary choices already present therein. This contrasts with security engineering concerns, which technical reasoning may suffice to substantiate, at least in some cases.

We see this with a few familiar examples: phones, personal computers (PCs),¹⁸ and video games. One clear strategy—arguably the only foolproof one—that would achieve the aim of protecting users from harms from third-party software would be to prevent phones from being able to download any software, and perhaps even bar them from the internet. Such an approach would, of course, undermine the functionality of the product and be a bad economic move. Existing smartphone providers strike different tradeoffs; none take an absolute approach.

Whereas PC operating systems (OSs) allow users to download almost anything, video-game consoles have much more stringent control over what is allowed on the machine. This is not because of fundamental security differences between PCs and Xboxes, but because the respective developers have chosen different tradeoffs between security, interoperation, and other interests.

PCs are key infrastructure for vast swaths of the economy and valued for versatile multi-purpose use. Exacting controls enacted by their manufacturers could make the devices undesirable and therefore not competitive in healthy market conditions, or, under monopoly conditions, deeply harm both users and the software industry. This is all the more so given historically permissive norms around what software can run on PCs.

In Section 4.2, we provide three case studies of security vetting concerns: app sideloading, alternative app stores, and browser engines (WebKit).

18. Throughout the paper, we use “PC” to refer personal computers. We do *not* use the narrower definition of PC as a personal computer compatible with the original IBM PC. In particular, we consider Macs to be PCs.

Hybrid Concerns. Finally, there are situations featuring aspects of both engineering concerns and vetting concerns, in which interoperation entails both the development of a secure system for interoperation and some sort of vetting of those developers looking to use that newly open system. In hybrid cases, third parties must still demonstrate that their products meet the requirements of an interoperation policy; at the same time, there is also engineering and collaboration needed to support technical interoperability.

Template of a Hybrid Concern

- 1) Interoperating would mean allowing third parties to access functionality reserved for only our use.
- 2) Opening those functionalities means third parties newly interacting with security-sensitive OS parts. Designing new systems to secure such access is a costly engineering task and may require innovation.
- 3) Therefore, third-party access to these functionalities carries inherent security risk, and could undermine the security of billions of users.

Perhaps surprisingly, by combining engineering and vetting considerations, hybrid cases often exhibit more complex dynamics than either alone, due to their interplay. The same powerful company plays two roles, platform gatekeeper in a vetting context, and necessary collaborator in an engineering context. Third party developers must liaise with this same company for both. For example, in opening mobile wallet functionality to third parties, device/OS providers need to both add APIs to allow developers access to previously restricted hardware and vet which developers will have access. Section 4.3 offers two case studies of hybrid concerns: NFC for payments and physical device interoperability.

The combination of these two roles in one entity expands its leverage beyond what might be expected from simply “interpolating” engineering and vetting concerns, rendering hybrid cases arguably the most interesting and complex of the three types. We discuss these relationships further, from an economic perspective, in Section 3.1.

Summary. Our Templates are designed to capture just the essential elements of the argument patterns we have identified. Of course, they are oversimplifications with respect to concerns being raised in any real-world context. Unsurprisingly, the arguments made in practice are more complex, and may not neatly fall into a single category.

Our case studies and analysis in Section 4–5 demonstrate the complexities of “security vs. interoperability” arguments in the wild, and show how recognizing the simple patterns identified in our taxonomy illuminates patterns that can inform critical evaluation of the security and economic aspects of real-world arguments in specific case study contexts.

3.1. Horizontal and Vertical Interoperation

Our taxonomy is closely correlated to distinctions in the relationships of the interoperating products—*horizontal* and *vertical* relationships—corresponding to similar terminology that often appears in economics and antitrust law.

To highlight this distinction, we define horizontal and vertical interoperation, generally in keeping with the use of these terms in [26]. In a nutshell, by *horizontal interoperation* we mean interoperation between products offered at the same level, whereas *vertical interoperation* is that between a platform or ‘higher layer’¹⁹ product and products that run *on* that platform or higher layer product.

Horizontal interoperation happens when similar products need to be made interoperable. Messaging is a good example, where previously competing products must collaborate on integrated functionality and security (Case Study 1). This happens when the products are *substitutable*, a term used in economics to mean two products used for similar purposes that compete for the same user demand [64].

Vertical interoperation happens between products on different layers. Instances of vertical interoperation that arise naturally (as opposed to through regulatory or antitrust enforcement) tend to be between some platform and a *complementary* product. Again using economic terminology, we say two products are *complementary* if they are often used together, or, formally, if a price increase of one decreases the demand for the other [64]. Smartphone apps are a good example, and the success of smartphones is greatly dependent on the wide availability of apps and other complementary products developed by third parties.

There is a clear incentive to achieve good vertical interoperation between platforms and the apps that run on them, as these products complement each other and increase customer utility in concert [71]. (Incentives in horizontal interoperation can be less cooperative.) Competitive friction in vertical interoperation may arise either from a platform maintaining extractionary practices (e.g., by taking commission on in-app purchases; see §4.2) or from a platform’s efforts to protect its own complementary, higher-layer product that is somehow privileged on its platform—this is called *self-preferencing* (e.g., payment apps having unique access to hardware functionality; see §4.3). The case where there is an in-house, higher-layer, complementary product with exclusive access to platform functionality, is a *hybrid* case in our taxonomy: the platform and the third-party product are complements, and the company’s higher-layer product is a substitute. This hybrid type of economic relationship where the platform is able to use its position to shut out other products is uniquely potent and the potential competitors are very vulnerable.

Relation to taxonomy. The economic context of horizontal or vertical interoperation may be useful to inform contextual analysis of SvI arguments. Security engineering arguments often relate to horizontal interoperation, and security vetting arguments are often, though not always,

19. We use ‘layers’ in a general sense here, not specifically those from the OSI model, but generally to mean products that run on other products.

related to vertical interoperation.²⁰ Figure 1 illustrates these correlations.

It makes sense that vetting concerns and vertical interoperation tend to be seen together as they both arise when one company has a platform with which others interoperate. The hybrid cases from our taxonomy are typically also situations in which third parties are pursuing interoperability on a company’s platform, so they are also more strongly associated with vertical interoperation.

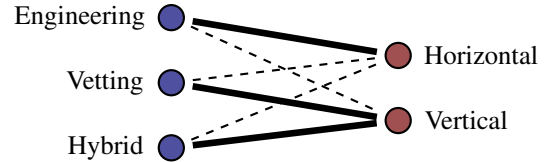


Figure 1. Our taxonomy and horizontal/vertical interoperation (strong/weak correlations in bold/dashed lines respectively)

Scope of our taxonomy. Our work focuses on security concerns in the context of adding interoperability to systems that previously had less or no support for interoperation. Some secure technologies have been designed to support open interoperation from the ground up, and some of the types of concerns discussed in this section will not arise at all in such cases. Interoperation between email providers (with PGP) is a good (horizontal) example; third-party software on Linux is a good (vertical) example illustrating that interoperation and security can be built from the ground up.²¹

4. Case Studies and Analysis

Based on recurring themes from the SvI discourse we reviewed, we propose four critical questions comprising an analytical framework for SvI concerns.

- 1) How do interoperation and economic incentives clash (or not)?
- 2) How do security arguments and economic incentives align (or not)?
- 3) What needs to change in order for the company to support interoperation?
- 4) What tension exists between security and other goals both before and after?

Next, for each taxonomy category—engineering (§4.1), vetting (§4.2), and hybrid (§4.3)—we provide 1–3 selected case studies, and analyze each case study with the four preceding questions in mind. Then in Section 5, we transition from individual case analysis to comparative analysis, structured around the same four questions.

4.1. Security Engineering Concerns

In security engineering cases, we have parties trying to build or retrofit their systems to work together. Picture

20. Theoretically, both types of arguments can arise in both horizontal and vertical interoperation scenarios. In practice, many complex real-world scenarios exhibit aspects of both, but the observation we wish to highlight is that there is a stronger correlation between certain categories.

21. Of course, PGP has well documented usability and other issues [30], [81]. Our point here is not to extol these examples’ security, but to contrast building in interoperation from the outset vs. retrofitting. See also Note 4 discussing how designing secure interoperation is hard.

dual-gauge trains with different wheel gauges being engineered to be able to operate (safely) on tracks of different width. In our cases, the companies involved are generally competitors and the interoperation is generally horizontal.

Case Study 1: E2EE Messaging. This case study discusses two examples of E2EE messaging, iMessage and WhatsApp, which involve distinct SvI considerations. Here, interoperation means that users of one service could send an end-to-end encrypted (E2EE) message to the users of a different E2EE service—while preserving security.²² We encountered mandated interoperability of Messenger (Meta) directly in our case search. There are also similar mandates for WhatsApp in the EU and iMessage in the US.²³ These cases have many similarities so we discuss them together. We found SvI arguments stating that interoperation is technically difficult and that third parties might not have adequate security guarantees [44], [69].

Before the actions of the antitrust authorities, WhatsApp and Messenger users could only message other users on WhatsApp and Messenger, respectively. WhatsApp has since taken limited measures to support interoperation; Messenger remains siloed. iMessage is only available on iPhones, but iMessage users could always send and receive (SMS) messages to and from Android phones.²⁴

There is substantial engineering work to be done to achieve secure interoperation across E2EE messaging applications—even for basic messaging functionality, putting aside common auxiliary features such as disappearing messages, read receipts, and so on. Meta’s encryption for both WhatsApp and Messenger is based on the Signal Protocol, which is developed by the non-profit Signal Foundation, and is considered the gold standard in the field [69]. Meta has stated a requirement that third parties seeking to interoperate must use the Signal Protocol or ‘a compatible protocol if they are able to demonstrate it offers the same security guarantees’ [69]. For smaller providers, the possibility of interoperating with WhatsApp may provide ample incentive to do the engineering work to meet these requirements. For Meta, secure interoperation will also require some engineering, including building secure connections with third-party servers and coordinating message formats [69].

In contrast, iMessage does not use the Signal protocol [59], and has sufficient market dominance that it may not be incentivized to either switch to the Signal protocol or otherwise facilitate interoperation. Historically, many communication protocols have been agreed upon by broad communities of users and operators, as with email. MLS, based on the Signal protocol, is an effort in that direction and we might eventually have a system of community standards for secure messaging. For now, the efforts for greater interoperation consist of some companies retrofitting interoperation conditional on adherence to their standards, and some community-led protocol development

efforts. There are serious technical and research challenges to interoperation, especially when it comes to the myriad of features available in modern messaging apps [25], [55].

For the incumbents, interoperation entails allowing their services to send and receive information outside of their own networks, and thereby potentially helping competitors. Major incumbent services are currently sufficiently popular that not allowing greater interoperation has been a boon—encouraging greater uptake—rather than a deterrent for customers (e.g., [43]). With the example of Apple and iMessage in particular, the incompatibility of messaging may play a role in users switching to iPhones because iMessage is only available on iPhones [41].

4.1.1. Analysis: Security Engineering Concerns.

1. How do interoperation and economic incentives clash (or not)? The incumbent companies currently appear to enjoy benefits from locking in users to their platforms (‘network effects’ [49]), which likely outweigh incentives to interoperate.²⁵ Apple can also bundle goods in a way that incentivizes exclusivity. The fact that iMessage is only available on iPhones and is not fully interoperable with messaging from Android phones [19] may further incentivize users to switch to iPhones. These incentives may lead companies to avoid full interoperation, rather than to enact exclusionary measures on competitors.

2. How do security arguments and economic incentives align (or not)? In many cases, interoperation may not be economically advantageous for the companies being asked to interoperate, as discussed above. For WhatsApp, opening up a closed system is not only an engineering challenge; it also means losing existing network effects. For iMessage, extensions to support full interoperation, including encryption, will be an engineering task and will remove an incentive for Android users to switch to iPhones. Here, however, there are also security arguments in the other direction: encrypting iMessage communications to/from Android better protects iMessage users. This is an interesting example of a company apparently eschewing security in favor of other economic incentives, yet at the same time framing some of their arguments for doing so as security arguments.

3. What needs to change in order for the company to support interoperation? Although Meta’s messaging apps already build on the Signal Protocol for WhatsApp, there is still a substantial amount of engineering to make sure that interoperation is secure. The Signal protocol is a centralized server design, the predominant paradigm in encrypted messaging, and Meta has also made some modifications to the Signal protocol in WhatsApp [69]. For Apple, some of the changes that are necessary for interoperation are simpler (such as chat bubble color [19]) whereas some are more complicated (such as encryption). In both cases, using community standards—such as Messaging Layer Security (MLS)—might achieve strong security for users and easier interoperation in the future.

4. What tension exists between security and other goals both before and after? End-to-end encryption is a well-researched goal, and there are standards bodies

22. REGULATION (EU) 2022/1925 on contestable and fair markets in the digital sector (Digital Markets Act), Article 7(3)

23. CASE (EU) DMA.100024 Meta – number-independent interpersonal communications services, 2023 and United States v. Apple, Inc., No. 2:24-cv-04055 (D.N.J. filed Mar. 21, 2024)

24. iMessage-to-iMessage communication offers end-to-end encryption and additional features not available in iPhone-to-Android communication on iMessage. Unlike iMessage, WhatsApp and Messenger do not support SMS messaging. The three apps are used for similar purposes in practice.

25. This appears likely from the companies’ resistance to recent interoperability mandates; see also, e.g., [43] for an empirical perspective.

and academic researchers as well as companies looking to improve the existing technology. There are serious open questions around how best to achieve interoperability in E2EE, especially between existing systems that need to be ‘retrofitted’ with interoperability capabilities; at the same time, there are viable avenues using existing technology to set up interoperability that remains secure [25], [55]. Thus, security considerations are not necessarily an insurmountable obstacle to an interoperability mandate in this context; at the same time, research progress over the course of the next few years may reveal ways to do interoperable E2EE much better. In the case of iMessage, interoperable encryption for communications with Android users will ultimately better protect Apple’s own users.

4.2. Security Vetting Concerns

Next, we present three similar relevant technologies, featuring distinct SVI concerns in the vetting category. All three case studies relate to Apple app stores as this has been the focus of EU efforts. There have been similar US cases against both Apple and Google (see Note 3).

We begin with some context. Apple has historically adhered to a ‘walled garden’ approach for iPhones. Users are only able to download and use apps vetted by Apple according to their security, privacy, and quality standards. The stringent screening of apps on the App Store has furthered the iPhone’s reputation for strong security [52].

This approach limits what users can do on their own mobile devices—far more strictly than on any existing PC systems.²⁶ Apple’s own approach on its Macs contrasts with its approach towards third-party software on its other devices. Apple has a notarization process for software intended for Macs, but this process is automated and much more limited than the process for iOS apps [9], [17]. It is also cheaper—the cost to developers for Macs is membership in the Apple Developer Program (99 USD yearly) [10], which iOS developers must have in addition to other substantial fees.²⁷ Once notarized, Mac software can be distributed via a website, not only via Apple marketplaces. These policies reflect Apple’s discretionary choices about tradeoffs between user choice and security vetting on different products.

From the perspective of developers and antitrust officials, there is another dimension to this tradeoff. Apple’s vetting of apps and its position as gatekeeper and security guarantor coincides with a position of market power. Apple’s control over its App Store allows it to determine what apps are offered and take a cut of transactions.

Thus, to cast security vetting concerns as only a balancing of user choice against security, is to miss the economic incentives at play. The core reasons behind the push towards more open app distribution appear to have been economic. Developers are not arguing for the freedom to distribute malware; rather, they want to avoid the substantial rents that gatekeepers force upon them.²⁸

Case Study 2: App Sideloading. App sideloading refers to downloading an app onto a device via some route other

than the official app store. This alternate route might be a website or alternative app store. Sideloading was not allowed on iPhones (or iPads) until the DMA, and is still not permitted outside the EU. Apple still requires that sideloaded apps be notarized, meaning the app is vetted and signed by Apple and only apps with such a signature can be downloaded onto a device. This notarization procedure is not as involved as the vetting for the App Store, but still includes all the security requirements in the App Store Guidelines [9]. A major reason why Apple says they need to notarize all apps, especially those with alternative distribution, is to maintain the security standards of apps on its App Store [35].

The notarization process is not necessarily cheaper than getting approved for the App Store, despite there being fewer requirements for Apple to check. Developers that choose sideloading must pay a 0.50 EUR ‘core technology fee’ (CTF) for each first annual install over one million, where annual installs include updates [14]. Apple allows free installs for a year by the same user, so within a year, the app can be updated multiple times for free; there is a charge to update each following year [22]. Updating apps to fix security issues is an important means of protecting users. As timely updates are important for security, disincentivizing proactive updates may undermine Apple’s stated goals of preserving security. Depending on a developer’s circumstances, this alternative pricing is not necessarily cheaper than the 30% cut Apple takes from the App Store and in-app purchases.²⁹ Apple justifies these fees by invoking the role it plays in developing tools for developers, which include security benefits from the notarization process [22], [23].

In addition to paying fees on purchases of apps, Apple requires all *in-app* purchases (IAP) of digital goods to be intermediated by Apple, and generally subjects these to a 30% fee [21] (this fee structure changed after the DMA in Europe, but remains in place elsewhere).³⁰ Outside the EU, Apple also forbids apps from linking to websites where purchases can be completed like any other online purchase (without Apple intermediating) [9]. Different rules govern the purchase of physical goods. The type of good (physical or digital) being purchased would appear to have no bearing on payment security. However, Apple’s justification for requiring usage of Apple’s IAP system is to ensure the security of transactions [35]. That said, intermediaries for processing payments securely online are common, and usually levy much smaller fees (e.g., Epic reports less than 5%).³¹

Case Study 3: Alternative App Stores. Apple must now allow alternative app stores, which will be able to distribute sideloaded apps. As discussed above, the apps being sideloaded must be notarized by Apple.

The alternative app store itself must abide by additional criteria set by Apple, which Apple can check before allowing the alternative marketplace to operate. Alternative marketplaces must, for example, agree not to

29. See Appendix for an example calculation of fees.

30. Even developers who choose a link out option now available in the EU still have to pay a 10-17% commission on sales of digital goods and provide Apple with transaction reports [18].

31. Epic Games, INC. v. Apple INC., Case 4:20-cv-05640-YGR, Findings of Fact and Conclusions of Law Proposed by Epic Games, Inc. 2021, §454

26. Recall that we use “PC” broadly to include Macs; see footnote 18.

27. See the Appendix for more on fees.

28. Epic Games, Inc. v. Apple Inc., Case 4:20-cv-05640-YGR, Findings of Fact and Conclusions of Law Proposed by Epic Games, Inc. 2021

distribute apps that infringe intellectual property rights or that are malicious as well as deal with requests for removal of apps by governments [13]. Apple also points out that collecting data about apps through its App Store is an important aspect of keeping users secure [35]. There is no reason that interoperability regulations would prevent Apple from engaging in or requiring this type of data sharing with alternative app stores [35]. Indeed, this type of data sharing would be beneficial even across existing marketplaces outside of Apple's control, e.g., Google Play.

The vetting concerns have been the prominent ones in these cases, but there are also engineering considerations involved. Apple created an API to allow these alternative marketplaces to be able to execute downloads [13]. There is also some extra work that needs to be done for developers distributing their apps via their website [20].

Case Study 4: WebKit. Prior to the DMA and the subsequent actions taken by the Commission, all web browser apps on iOS had to use WebKit as their browser engine [6]. Browser engines are part of web browser apps (and in-app browsing) that render the content of a website into a page ready for user interaction [58]. WebKit is open source, but belongs to Apple [79]. As a result of Commission actions, Apple now allows alternative browser engines, only in the EU, both for browser apps and in-app browsing [7]. Prior to these changes, Apple's iOS was the only operating system that did not support other browser engines; other browser engines can be used on the operating systems of their competitors [76]. In the developer documentation, the requirement that browsers use WebKit is not explicitly based on security, although there is notable community discussion around security motivations for this requirement [67].

Browser engines play a key role in preserving security for users online. Here, iOS users may be disadvantaged by the scarcity of options available [61]. WebKit has not been demonstrated to be, and does not have a strong reputation for being, any more secure than other browser engines [61]. There have been bugs in WebKit and Safari [58], and not allowing developers (of browsers or those using in-app browsing) to use the tools they see fit could constrain their ability to make application-specific security choices.

Apple stipulates that any developer looking to use an alternative browser engine must meet certain requirements, including some related to security [7]. Any browser app would also have to abide by Apple's general app guidelines, including those regarding security [9]. Any developers looking to implement an alternative browser engine must be approved by Apple, allowing Apple to vet potential alternatives and protect users from insufficiently secure options [7].

4.2.1. Analysis: Security Vetting Concerns.

1. How do interoperation and economic incentives clash (or not)? The three case studies share the important context of Apple's control over third-party developers' access to their potential customer base on the iPhone. iPhone and iOS comprise a relatively closed device and platform ecosystem, and Apple can exclude developers on grounds that their apps do not meet Apple's guidelines or because their services are not allowed in the ecosystem (e.g., alternative app stores). Apple's monopolistic

position definitionally also allows it to charge developers more than would be expected in more competitive settings. This type of 'gatekeeper' power differs markedly from the market power discussed in the security engineering case study above, and in horizontal interoperation more generally. Here, Apple has the power to completely exclude a third party; in horizontal interoperation, it cannot cleave third-party developers from users.

2. How do security arguments and economic incentives align (or not)? Vetting apps to protect user security is a reasonable end, but it is also used as a means to extract rents. Keeping malware and other insecure apps away from users is also good for platforms, especially those that, like Apple, enjoy a reputation for security and good curation [52]. It is hard to (externally) evaluate whether the price tag is justified, given system opacity and limited competition.

3. What needs to change in order for the company to support interoperation? In all these cases, some amount of vetting is important to preserve the security status quo. Apple's notarization system and CTF is Apple's suggested way forward. As discussed above, the notarization guidelines are less onerous for Apple to check than their status quo, and vetting new app stores will likely be a much rarer occurrence than vetting new apps—but Apple's new mechanisms are not necessarily cheaper for developers. There have been changes to Apple's pricing practices (and it is possible more changes will need to be made in the future). Price changes might be impactful for the company's profits, but changing pricing is typically not an engineering challenge.

4. What tension exists between security and other goals both before and after? Apple has absolute control over third-party developer access to iPhone users. At the same time, they rely on those third parties to develop apps for the iPhone, increasing the iPhone's utility and commercial success. The ecosystem of iOS apps is massive, and preventing every possible 'bad' outcome is too general and too far-reaching to be a viable reality. Instead, Apple has policies (e.g., [9]) around how they protect users and devices 'well enough.' Inherent in these policies are tradeoffs around security, safety, privacy, and quality. Too-stringent guidelines might unnecessarily limit available apps or take too many resources. Too-lenient guidelines might undermine user trust and device integrity.

The changes the Commission is enforcing will not necessarily impose new tradeoffs when it comes to app vetting. Apple itself decided to apply only a subset of app guidelines to those apps applying for notarization (whether for economic reasons or otherwise). Alternative app payments and alternative app stores will require users to invest their trust in other third parties. Then, choosing an acceptable tradeoff falls in larger part to the users; they must choose which companies' security (and privacy) policies are trustworthy and/or worth the risk.

4.3. Hybrid Concerns

Recall that hybrid cases are those in which the company is opening up a functionality to third parties that was previously only available to its own in-house product. To do this, it must engineer a system that can preserve

security when opened up to third parties, as well as vet those third parties.

Case Study 5: NFC for mobile payments. We identified Near Field Communication (NFC) as a relevant technology from both the Apple Mobile Payments antitrust case³² and the Qualcomm/NXP Semiconductors merger.³³ The Qualcomm/NXP Semiconductors merger mandated interoperation between NFC chips and other chips whereas the Apple case mandates interoperation between those types of chipsets and software. (There is also a similar NFC-related antitrust proceeding in the US against Apple.)³⁴ In our search for SvI concerns, we did not find any articulated concerns regarding the merger so we focus on the Apple case. The ‘security vs. interoperability’ considerations discussed by Apple include that new APIs had to be built to allow third-party developers secure access to the technology *and* that those developers will be vetted before such functionality is available [12], which falls into our hybrid definition.

NFC is a set of protocols that work at close range and allow two devices to communicate securely. NFC is used for myriad applications linking smartphones to other devices, including reading tags on objects, serving as keys, or communicating credit card or identification information [11]. For an app to use NFC for mobile payments, it must have access to the NFC antenna in the phone. It must also access key information that is stored on the Secure Element, which holds sensitive information, including the card information necessary for host card emulation (HCE) [8]. Apple had restricted third parties from using NFC and the Secure Element for HCE, reserving this ability for Apple Wallet and Apple Pay. It did allow other usage of NFC via API access to the necessary hardware and software [15].

EU antitrust authorities identified this as monopolistic behavior and Apple has opened up the HCE capability to third-party apps, subject to approval by Apple. The approval criteria require third-party developers to commit to complying with laws and standards related to privacy and security, including standards set by EMVCo, a standards body for card-based payments [15]. In addition, Apple requires third-party developers to have certain policies around privacy and dealing with vulnerabilities [15]. This is a vetting concern, and screening developers seeking to use HCE is an important aspect of protecting security in the newly open system.

In order to ‘open up’ NFC capabilities for third-party wallet applications, third-party developers must have access to NFC, which is already available, as well as access to the Secure Element [12].³⁵ Access to the Secure Element is already separate from the Secure Enclave, which is where the operating system stores other sensitive data [11]. This new access must be built correctly in order to preserve the security of both the third-party data and

the rest of the system. The Secure Element has internal security boundaries that could impede a malicious developer from accessing other sensitive data and none of this data needs to come into contact with the operating system or app—the reply can go straight from the hardware to the payment processor [31]. Thus, APIs built for third-party developers could grant access to only specific functionalities without compromising others. There are also existing vulnerabilities in these products [31], which would not necessarily be exacerbated by interoperability and might benefit from greater attention from the community. Thus, there are a range of security engineering security concerns to be solved by Apple.

Case Study 6: OS and Physical devices. We identified OS and physical device interoperation as a type of relevant technology from three cases: two similar cases involving Apple’s iOS³⁶ and the Google/Fitbit merger.³⁷ The Apple cases concern the interoperability between many aspects of iOS and third-party hardware and software whereas the merger focuses on the interoperation between specific third-party hardware and the Android OS. (The US case concerning NFC, mentioned above,³⁸ also discusses physical device interoperation in a similar light to the EU cases about Apple.) The SvI arguments regarding the Apple cases are exemplified in a whitepaper by Apple [16].

Public discussions about security in the Google/Fitbit merger case were notably very different; they did not discuss the security of the *mandated* interoperability, but rather discussed distinct *voluntary* interoperability that would result from the merger, reassuring users that it would not endanger user security or privacy [65]. This type of argument is outside our current scope, so we focus on the Apple case for the rest of the case study. However, investigating this type of ‘inverted’ case—and examining how perspectives on the the compatibility of security and interoperability feature differently across economic contexts—could make for interesting future work.

The Apple cases cover many different hardware and software features of iOS, including notifications on smartwatches, background execution, content casting and transfers, and paired device set up. Apple will be required to provide interoperability with the full list of functionalities to third parties. All of these functionalities are already available to Apple’s own devices (including Apple Watch, AirPods, and other iPhones), so achieving interoperability is a question of opening up previously reserved functionality to third parties, generally via APIs and SDKs.

Although the stipulations from the Commission are still evolving, Apple is currently evaluating interoperability requests on a case-by-case basis [16]. In their recent public-facing document, Apple mentions that Meta has made 15 requests for interoperation regarding various functionalities [16]. While Apple may be required to interoperate with competitors, the regulators do not require that any interoperation request be granted in a way that would undermine the security of the device.³⁹ Thus, Apple could

32. CASE (EU) AT.40452 Apple - Mobile Payments

33. CASE (EU) M.8306-QUALCOMM / NXP SEMICONDUCTORS

34. *United States v. Apple Inc.* 2:24-cv-04055 (JXN-LDW) (D.N.J.)

35. Android supports HCE both with and without a secure element, and allows third-party interoperation with the latter method; third-party Android developers cannot access the secure element [5]. If Apple adopted a similar approach, it could potentially achieve interoperability without involving the secure element at all; it has not opted for this approach.

36. CASE (EU) DMA.100204 SP - Apple - Article 6(7) – process and CASE (EU) DMA.100203 Apple – Operating systems – iOS – Article 6(7) – SP – Features for Connected Physical Devices

37. CASE (EU) M.9660 GOOGLE/FITBIT

38. *United States v. Apple Inc.* 2:24-cv-04055 (JXN-LDW) (D.N.J.)

39. REGULATION (EU) 2022/1925 on contestable and fair markets in the digital sector (Digital Markets Act), Article 6(7)

deny interoperation requests from known malicious actors and develop/require bespoke solutions for interoperation to reduce security risk.

One example is peer-to-peer (P2P) Wi-Fi connections, which can be used to transfer files, such as with Apple's AirDrop, and continuity services, such as Handoff or Universal Clipboard [73]. These functionalities use a Bluetooth Low Energy (BLE) connection between two devices to create an *ad hoc* P2P Wi-Fi connection, which uses Apple's iCloud credentials as part of its certificate procedure [11]. Several aspects of these services, including BLE, have been shown to leak user information or otherwise have vulnerabilities [28], [47], [62]. Apple Wireless Direct Link (AWDL) is an key protocol used in P2P Wi-Fi, which is based on IEEE 802.11, a set of standards, but is currently proprietary [74]. This protocol has been shown to have security vulnerabilities [73]–[75]. AWDL being proprietary is a barrier both to better study of its security and to interoperation [74].

To open P2P Wi-Fi up more broadly, the Commission proposes⁴⁰ that Apple either make AWDL available to third parties or facilitate third-party interoperation through Wi-Fi Aware,⁴¹ which is a public protocol with similar functionality that is based on AWDL [29]. If Apple makes AWDL public, there is little engineering to be done, if the protocol is indeed secure. If the security of AWDL is reliant upon its details remaining secret, i.e. *security through obscurity*, Apple and its users might be better served by Wi-Fi Aware or an improved version of AWDL.

4.3.1. Analysis: Hybrid Concerns. The hybrid cases are more than just the sum of the other two; we see (arguably more complex) patterns specific to this category.

1. How do interoperation and economic incentives clash (or not)? The platform's market power is again a key feature of these cases. Since third-party products compete directly with those of the incumbent company (e.g., Apple Watch competing with third-party watches), the company has incentive to protect their current market share. At the same time, the company has control over access to those key functionalities and can block access for competitors. In contrast to vetting concerns, interoperation means that third parties gain access to functionality that was not previously available to third-party developers at all. Since the company must both build access to previously exclusive functionality and also vet who gets that access, the platform's control over the situation is broader than in either engineering or vetting cases. Thus, the company's ability to block access may be more robust in the hybrid case.

2. How do security arguments and economic incentives align (or not)? The platform has a clear economic incentive to protect their exclusive products that are bundled with or complementary to their main devices. Preventing third-party developers from offering the full functionality available on Apple's own products reduces the value of those other products and puts theirs at an advantage, i.e., self-preferencing. Supporting interoperation would require security engineering in concert with third parties. These

incentives may coalesce into significant motivation for a platform to keep systems closed.

3. What needs to change in order for the company to support interoperation? Not only must the platform build secure APIs or other means of access for third-party developers, but many of these APIs may need to be bespoke for specific uses. This could be a significant engineering task. The platform can vet all proposals for interoperation; this enables them to enforce security standards, and keep tabs on what third-party developers are doing. Given the previously exclusive nature of the functionality opened up, interoperation in hybrid cases may be subject to more scrutiny from the platform in control than in vetting cases, and may require more coordination between the platform and third parties. Although perhaps costly, this may make for better, more secure products.

4. What tension exists between security and other goals both before and after? Existing interoperation policy involves interoperation with third parties, despite some potential risks (such as with Bluetooth devices [32]). When opening interoperation, the platform's greater case-by-case control in hybrid cases may mean less difficulty in maintaining security standards than when having to vet millions of apps as in the pure vetting case.

5. Comparative Analysis and Takeaways

We now offer a *comparative* analysis, identifying key considerations across our taxonomy and case studies. First, we consider *economic incentives, market power, and security*, corresponding to Analysis Questions 1 and 2. Then we discuss *security trade-offs*, corresponding to Analysis Questions 3 and 4. Finally, we offer big-picture takeaways. Table 3 (Appendix) provides a succinct summary of our comparative analysis.

Economic incentives, market power, and security. Recognizing the nature of a company's market power can be a key step in understanding the ways in which security can become subordinated to other business goals. There are two main types of market power that are relevant in the cases we discuss: regular market dominance, where a company is simply so large it dominates some market; and platform power, where incumbent companies are 'gatekeepers' of third parties' access to customers. We did not specifically categorize cases by the nature of the incumbent company's market power, and yet different security concerns seem to correlate with different types of market power. Cases with *security engineering concerns* are also those in which the market power of the incumbent is simply *market dominance*. The relative size of a company, or, more precisely, its market share, and the resultant network effects, can confer significant power without more complicated 'gatekeeper' dynamics. As noted in Section 3, these instances are also often those in which the necessary interoperation is horizontal, meaning third parties might be on a more equal footing when it comes to making technical decisions. Interoperating securely is generally an engineering task to be coordinated between the companies involved and, if there are existing standards, it is clear what it takes to 'interoperate securely.' We can see *platform power* clearly in *security vetting concerns*, which are also instances of vertical interoperation. As noted in

40. DMA.100203 – Article 6(7) – Apple – iOS – SP – Features for connected physical devices

41. Also called Neighbor Awareness Networking (NAN).

Section 4, vetting concerns involve company discretion regarding security policy choices, and rarely have clear-cut engineering answers. As such, we view narratives around vetting concerns as potentially more easily tailored to fit a company’s economic needs. The platform position in these cases typically gives the company significant power to impose potentially punitive prices or exclude third-party developers. Thus, this type of concern should be identified as particularly susceptible to a blurring of boundaries between security and economic incentives, compared to engineering concerns. The *hybrid case* is not simply a dilution of the dynamics of the other two cases. *Platform power* manifests here too. Rather than using platform power to extract fees, as with security vetting concerns, hybrid cases more often feature or involve risks of companies using their platform power for self-preferencing their products, hobbling or entirely excluding potential competition. In both vetting and hybrid cases, the company acts as a gatekeeper. The extensive control of incumbent companies to block competition through both vetting and engineering is distinct to hybrid cases, meaning platform power is particularly entrenched.

The engineering demands in a hybrid case appear in general to be no less significant than in a security engineering case. Thus, platform power is bolstered by legitimate engineering concerns. This means there are two lines of defense to keep out both bad actors and competitors, compounding the effects we see in pure engineering or vetting cases. Third-party competitors may be more completely shut out in hybrid cases as compared to the other two categories. Without interoperation, messaging apps can still function with their own users, and apps can be distributed on iPhones as long as they adhere to Apple’s guidelines and fee schemes. But without access to the HCE, there can be no alternative to Apple Pay on the iPhone. Third-party smartwatches can function without access to all hardware functionalities, but their utility may be significantly limited. Thus, hybrid security concerns should be evaluated with careful consideration of these multi-faceted market ramifications as compared to engineering or vetting concerns.

Security tradeoffs. Security engineering involves many practical tradeoffs: between security and efficiency, usability, profit, and more. Achieving usability and security at once is well known to be challenging [34]. Usability also interacts with companies’ economic incentives: a phone with such tight security that it is unusable would be hard to sell. Economic interests can also motivate pressures against interoperation. Just as undermining usability through a narrow focus on security can ruin a product, undermining competition through a narrow focus on security can ruin a market. The simplest case is again the *security engineering concern*. Inherent in the idea of an engineering concern is the idea that the problem can be solved by engineering. The tradeoff, then, relates to how much to invest in solving the engineering problem and how much of a burden that is. In practice, of course, even the best, well-funded systems have bugs and vulnerabilities. Thus, companies must deploy systems that might be vulnerable. This tension carries over into interoperation, where, as in most other contexts, systems might have vulnerabilities despite their best efforts.

When companies raise *security vetting concerns*, they may argue that security considerations necessitate limitations on interoperation, or perhaps preclude interoperation entirely. Recall that vetting is about *interoperability policies*, rather than *technical interoperability*. Policies generally involve discretionary tradeoffs between security and other interests. The tradeoffs made in existing policies are an essential reference to evaluate how much of a divergence from existing security practices, and how much of an economic burden, a proposed policy change would be. The *hybrid case* may feature all of the preceding types of tradeoffs. Yet the hybrid tradeoffs are of a slightly different character than the engineering and vetting tradeoffs. Those seeking to interoperate with OS functionality reserved for device manufacturer use are fewer than those seeking to make apps for smartphones, so vetting could be a project of a substantially smaller scale. Relatedly, interoperation could be bespoke, involve more monitoring, and require less scalability.

Big picture. Our taxonomy, case studies, and analysis highlight how the following prominent themes feature in ‘security vs. interoperability’ discourse in impactful competition policy contexts in the wild.

- 1) Interoperation and economic incentives often conflict.
- 2) Security arguments and economic incentives often align.
- 3) Such security arguments and their implications can only be fully understood in the broader economic and policy context as well as the technical security context.

Where vetting is the primary security concern, incumbent companies necessarily make tradeoffs and also have strong platform control that can be leveraged to extract fees. The hybrid combination of platform power and guarded functionality can grant incumbent companies even more power to exclude direct competition.

6. Conclusion

We have presented a systematization of “security vs. interoperability” arguments based on an analysis of relevant EU cases. We offer a taxonomy, a analytical framework, and case studies of the diverse contexts in which SvI arguments arise; our comparative analysis underscores their distinguishing characteristics.

Court proceedings and regulatory investigations in the area will continue to be common [72]. Many of the investigations we mention are ongoing (e.g., [38]). We hope our contributions provide an actionable framework for the security community’s deeper interdisciplinary engagement with lawyers, regulators, and policymakers to clarify and mitigate potential security harms in the context of antitrust.

Acknowledgments

The authors would like to extend special thanks to Mallory Knodel for helpful discussion and many insights. We are also grateful for the generous help of Alexander Heinrich, who provided detailed consultation on certain technical issues. Thanks also to Michael A. Specter, Stephanie Chen, Kyle Hogan, Andrés Fábrega, and Mathy Vanhoef.

References

- [1] RFC 9420: The messaging layer security (MLS) protocol. IETF.
- [2] ANDERSON, R. Why information security is hard-an economic perspective. In *Seventeenth Annual Computer Security Applications Conference* (01 2002), pp. 358 – 365.
- [3] ANDERSON, R. *Security Engineering, 3rd Edition*, 3rd edition. ed. Wiley, 2020.
- [4] ANDERSON, R. J., AND MOORE, T. Information security economics - and beyond. In *Advances in Cryptology - CRYPTO 2007, 27th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2007, Proceedings* (2007), A. Menezes, Ed., vol. 4622 of *Lecture Notes in Computer Science*, Springer, pp. 68–91.
- [5] ANDROID. Host-based card emulation overview. Android Developers, 2024. Permalink: <https://perma.cc/CGA5-NLXL>, URL: <https://developer.android.com/develop/connectivity/nfc/hce>.
- [6] APPLE. App review guidelines. Apple Developer Resources. Section 2.5.6, Permalink: <https://perma.cc/WL67-ZYUH>, URL: <https://developer.apple.com/app-store/review/guidelines/>.
- [7] APPLE. Using alternative browser engines in the European Union. Apple Developer Resources. Permalink: , URL: <https://developer.apple.com/support/alternative-browser-engines/>.
- [8] APPLE. How Apple Pay keeps users’ purchases protected. Apple Platform Security, 2021. Permalink: <https://perma.cc/9WBC-QMDA>, URL: <https://support.apple.com/en-gb/guide/security/secb53a35f0/web>.
- [9] APPLE. App review guidelines, 2024. Permalink: <https://perma.cc/C5UG-8ZQG>, URL: <https://developer.apple.com/app-store/review/guidelines/>.
- [10] APPLE. Apple developer program license agreement, 2024. Permalink: <https://perma.cc/P7T3-CELL>, URL: <https://developer.apple.com/support/terms/apple-developer-program-license-agreement/#ADPLA6.1>.
- [11] APPLE. Apple platform security, 2024. Permalink: <https://perma.cc/Z4F5-HVJ8>, URL: https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf.
- [12] APPLE. Developers can soon offer in-app NFC transactions using the Secure Element. Apple Newsroom, 2024. Permalink: <https://perma.cc/LJ9Q-G4WE>.
- [13] APPLE. Getting started as an alternative app marketplace in the European Union. Apple Developer Resources, 2024. Permalink: <https://perma.cc/U6VL-959G>, URL: <https://developer.apple.com/support/alternative-app-marketplace-in-the-eu/>.
- [14] APPLE. Getting started with web distribution in the EU. Apple Developer Resources, 2024. Permalink: <https://perma.cc/5ZGR-736K>, URL: <https://developer.apple.com/support/web-distribution-eu/>.
- [15] APPLE. HCE-based contactless NFC transactions for apps in the European Economic Area (EEA). Apple Developer Support, 2024. Permalink: <https://perma.cc/G4A6-DSRN>, URL: <https://developer.apple.com/support/hce-transactions-in-apps/>.
- [16] APPLE. It’s getting personal., 2024. Permalink: <https://perma.cc/AW34-KRYW>, URL: <https://developer.apple.com/support/downloads/DMA-Interoperability-Dec-2024.pdf>.
- [17] APPLE. Notarizing macOS software before distribution. Apple Developer Documentation, 2024. Permalink: <https://perma.cc/7X5E-SK9D>, URL: <https://developer.apple.com/documentation/security/notarizing-macos-software-before-distribution>.
- [18] APPLE. Using alternative payment options on the App Store in the European Union. Apple Developer Resources, 2024. Permalink: <https://perma.cc/7CVJ-XCR3>, URL: <https://developer.apple.com/support/apps-using-alternative-payment-providers-in-the-eu/>.
- [19] APPLE. What is the difference between iMessage, RCS, and SMS/MMS? Apple Support, 2024. Permalink: <https://perma.cc/D2T4-6W6W>, URL: <https://support.apple.com/en-us/104972>.
- [20] APPLE. Distributing your app from your website. Apple Developer Support, 2025. Permalink: <https://perma.cc/HL9D-XX6K>, URL: <https://developer.apple.com/documentation/appdistribution/distributing-your-app-from-your-website>.
- [21] APPLE. Membership details. Apple Developer Program, 2025. Permalink: <https://perma.cc/9TJS-96E2>, URL: <https://developer.apple.com/programs/whats-included/>.
- [22] APPLE. Understanding the core technology fee for ios and ipados apps in the european union. Apple Developer Support, 2025. Permalink: <https://perma.cc/3T9J-9P2E>, URL: <https://developer.apple.com/support/core-technology-fee/>.
- [23] APPLE NEWSROOM. Apple announces changes to iOS, Safari, and the App Store in the European Union, 2024. Permalink: <https://perma.cc/Z25U-UKGX>.
- [24] BIETTI, E. Explainer: Competition, Data and Interoperability in digital markets | Privacy International. Privacy International.
- [25] BLESSING, J., AND ANDERSON, R. One protocol to rule them all? On securing interoperable messaging. In *Security Protocols XXVIII* (Cham, 2023), F. Stajano, V. Matyáš, B. Christianson, and J. Anderson, Eds., Springer Nature Switzerland.
- [26] BOURREAU, M. DMA: Horizontal and vertical interoperability obligations. Centre on Regulation in Europe (CERRE), 2022.
- [27] BUTERIN, V. Onward from the hard fork, 07 2016.
- [28] CELOSIA, G., AND CUNCHE, M. Discontinued privacy: Personal data leaks in Apple bluetooth-low-energy continuity protocols. *Proceedings on Privacy Enhancing Technologies 2020* (12 2019).
- [29] CHESHIRE, S. D. Proximity Wi-Fi, U.S. Patent US20180083858A1, Mar. 2018. assignee: Apple Inc.
- [30] CLARK, J., VAN OORSCHOT, P. C., RUOTI, S., SEAMONS, K., AND ZAPPALA, D. SoK: Securing email—a stakeholder-based analysis. In *Financial Cryptography and Data Security: 25th International Conference, FC 2021* (2021), p. 360–390.
- [31] CLASSEN, J., HEINRICH, A., REITH, R., AND HOLLICK, M. Evil never sleeps: When wireless malware stays on after turning off iPhones. In *Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks* (May 2022), WiSec ’22, ACM, p. 146–156.
- [32] CLASSEN, J., AND HOLLICK, M. Happy MitM: fun and toys in every bluetooth device. In *Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks* (June 2021), WiSec ’21, ACM, p. 72–77.
- [33] COHEN, J. *Between Truth and Power: The Legal Constructions of Informational Capitalism*. Oxford University Press, 10 2019.
- [34] CRANOR, L. F., AND GARFINKEL, S. *Security and Usability: Designing Secure Systems that People Can Use*. O’Reilly Media, 2005.
- [35] DAVIS, G. Complying with the digital markets act. Apple, 2024. Permalink: <https://perma.cc/2KRG-LQ59>, URL: <https://developer.apple.com/security/complying-with-the-dma.pdf>.
- [36] ELECTRONIC PRIVACY INFORMATION CENTER. FBI v. Apple. <https://epic.org/documents/apple-v-fbi-2>.
- [37] EU COMMISSION. Competition case search. URL: <https://competition-cases.ec.europa.eu/search>.
- [38] EU COMMISSION. Commission closes investigation into Apple’s user choice obligations and issues preliminary findings on rules for alternative apps under the Digital Markets Act. Press Release, 2025. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1086.
- [39] EUROSTAT. NACE rev. 2 statistical classification of economic activities in the European Community. Methodologies and Working papers. ISSN 1977-0375.
- [40] FIDLER, M. Cybersecurity Mission Creep, Sept. 2023. draft on file with authors.
- [41] FOX, M. DOJ v. “The Blue Bubble”. Corporate and Business Law Journal, 2024.
- [42] FRISCHMANN, B. M., AND VAN SCHEWICK, B. Network Neutrality and the Economics of an Information Superhighway: A Reply to Professor Yoo. *Jurimetrics*, Vol. 47, Sept. 2007.
- [43] GARCIA-SWARTZ, D. D., MUHAMEDAGIĆ, M., AND SAENZ, D. The role of prices and network effects in the growth of the iphone platform. *Technological Forecasting and Social Change* 147 (2019), 110–122.

- [44] GREENBERG, A., AND COUTS, A. The DOJ Puts Apple's iMessage Encryption in the Antitrust Crosshairs. *Wired*, 2024. Permalink:<https://perma.cc/B8X5-QPXJ>, URL: <https://www.wired.com/story/apple-doj-antitrust-imessage-encryption/>.
- [45] GROSS, S. R. Expert evidence. *Wisconsin Law Review* (1991).
- [46] HALPIN, H. Sok: why johnny can't fix PGP standardization. In *ARES 2020: The 15th International Conference on Availability, Reliability and Security, Virtual Event, Ireland, August 25-28, 2020* (2020), M. Volkamer and C. Wressnegger, Eds., ACM, pp. 34:1–34:6.
- [47] HEINZE, D., CLASSEN, J., AND HOLLICK, M. ToothPicker: Apple picking in the iOS bluetooth stack. In *14th USENIX Workshop on Offensive Technologies (WOOT 20)* (Aug. 2020), USENIX Association.
- [48] HOVENKAMP, H. Antitrust Interoperability Remedies. U of Penn, Inst for Law & Econ Research Paper No. 22-14, Jan. 2023.
- [49] JULLIEN, B., PAVAN, A., AND RYSMAN, M. Two-sided markets, pricing, and network effects. In *Handbook of Industrial Organization, Volume 4*, K. Ho, A. Hortaçsu, and A. Lizzeri, Eds., vol. 4 of *Handbook of Industrial Organization*. Elsevier, 2021, pp. 485–592.
- [50] KADES, M., AND MORTON, F. S. Interoperability as a competition remedy for digital networks. *Equitable Growth*.
- [51] KANG, C. Net neutrality rules struck down by appeals court. *New York Times*, 2025. <https://www.nytimes.com/2025/01/02/technology/net-neutrality-rules-fcc.html>.
- [52] KNEZEVIC, O. Android vs iPhone security: which is safer? Norton Blog, 2024. Permalink:<https://perma.cc/TE3C-HHE3>, URL: <https://us.norton.com/blog/mobile/android-vs-ios-which-is-more-secure>.
- [53] KOTZIAS, P., RAZAGHPANAH, A., AMANN, J., PATERSON, K. G., VALLINA-RODRIGUEZ, N., AND CABALLERO, J. Coming of age: A longitudinal study of TLS deployment. In *Proceedings of the Internet Measurement Conference 2018, IMC 2018, Boston, MA, USA, October 31 - November 02, 2018* (2018), ACM, pp. 415–428.
- [54] LEMLEY, M. A., AND SAMUELSON, P. Interfaces and Interoperability After Google v. Oracle. *Texas Law Review* (Nov. 2021).
- [55] LEN, J., GHOSH, E., GRUBBS, P., AND RÖSLER, P. Interoperability in end-to-end encrypted messaging. *Cryptology ePrint Archive*, Paper 2023/386, 2023.
- [56] LENAERTS, K., GUTMAN, K., AND NOWAK, J. T. *EU Procedural Law*. Oxford European Union Law Library, 2023.
- [57] LIAN, W., RESCORLA, E., SHACHAM, H., AND SAVAGE, S. Measuring the practical impact of DNSSEC deployment. In *22nd USENIX Security Symposium (USENIX Security 13)* (Washington, D.C., Aug. 2013), USENIX Association, pp. 573–588.
- [58] LIM, J., JIN, Y., ALHARTHI, M., ZHANG, X., JUNG, J., GUPTA, R., LI, K., JANG, D., AND KIM, T. SoK: On the analysis of web browser security, 2021.
- [59] LINKER, F., SASSE, R., AND BASIN, D. A formal analysis of apple's iMessage PQ3 protocol. *Cryptology ePrint Archive*, Paper 2024/1395, 2024.
- [60] LOO, R. V. Privacy pretexts. *Cornell Law Review* 1 108 (2022).
- [61] LUO, M., LAPERDRIX, P., HONARMAND, N., AND NIKIFORAKIS, N. Time does not heal all wounds: A longitudinal analysis of security-mechanism support in mobile browsers. In *Network and Distributed System Security (NDSS) Symposium* (01 2019).
- [62] MARTIN, J., ALPUCHE, D., BODEMAN, K., BROWN, L., FENSKE, E., FOPPE, L., MAYBERRY, T., RYE, E., SIPES, B., AND TEPOV, S. Handoff all your privacy – a review of Apple's bluetooth low energy continuity protocol. *Proceedings on Privacy Enhancing Technologies* 2019 (10 2019), 34–53.
- [63] MUELLER, F. Harvard and Georgia Tech professors debunk Apple's security pretext for App Store monopolism: Epic Games v. Apple. *Foss Patents*, 2021. Permalink: <https://perma.cc/GX96-H5H8>, URL: <http://www.fosspatents.com/2021/03/harvard-and-georgia-tech-professors.html>.
- [64] NICHOLSON, W., AND SNYDER, C. *Microeconomic Theory*. Thomson South-Western, 2008.
- [65] OSTERLOH, R. Google completes fitbit acquisition. Google, 2021. Permalink:<https://perma.cc/52UF-Z4GC>, URL: <https://blog.google/products/platforms-devices/fitbit-acquisition/>.
- [66] PARK, S., SPECTER, M. A., NARULA, N., AND RIVEST, R. L. Going from bad to worse: from internet voting to blockchain voting. *J. Cybersecurity* 7, 1 (2021).
- [67] R/IOS. Is there any actual reason why Apple doesn't allow any other browser engines other than WebKit on iOS/iPadOS. Reddit, 2023. https://www.reddit.com/r/ios/comments/18trk72/is_there_any_actual_reason_why_apple_doesnt_allow/.
- [68] ROZENSHTEIN, A. Surveillance intermediaries. *Stanford Law Review* 70 (01 2018), 99–189.
- [69] SECURITY. Making messaging interoperability with third parties safe for users in Europe. Engineering at Meta, 2024. Permalink: <https://perma.cc/57JX-DCKN>, URL: <https://engineering.fb.com/2024/03/06/security/whatsapp-messenger-messaging-interoperability-eu/>.
- [70] SHANOR, A. The new Lochner. *Wisconsin law review* 2016 (01 2016), 133–208.
- [71] SINGH, A., HOSANAGAR, K., AND NEVO, A. Network externalities and app store fees in mobile platforms, 2021. Preprint available at SSRN.
- [72] STOLTON, S. Apple, google defeats to fuel EU's crackdown on big tech. *Bloomberg*, 2024.
- [73] STUTE, M., HEINRICH, A., LORENZ, J., AND HOLLICK, M. Disrupting continuity of apple's wireless ecosystem security: New tracking, DoS, and MitM attacks on iOS and macOS through bluetooth low energy, AWDL, and Wi-Fi. In *30th USENIX Security Symposium (USENIX Security 21)* (Aug. 2021), USENIX Association, pp. 3917–3934.
- [74] STUTE, M., KREITSCHMANN, D., AND HOLLICK, M. One billion apples' secret sauce: Recipe for the Apple Wireless Direct Link ad hoc protocol. *CoRR abs/1808.03156* (2018).
- [75] STUTE, M., NARAIN, S., MARIOTTO, A., HEINRICH, A., KREITSCHMANN, D., NOUBIR, G., AND HOLLICK, M. A billion open interfaces for eve and mallory: MitM, DoS, and tracking attacks on iOS and macOS through apple wireless direct link. In *28th USENIX Security Symposium (USENIX Security 19)* (Santa Clara, CA, Aug. 2019), USENIX Association, pp. 37–54.
- [76] THE COMPETITION AND MARKETS AUTHORITY. Mobile browsers and cloud gaming market investigation, WP2: The requirement for browsers operating on iOS devices to use Apple's WebKit browser engine. The Competition and Markets Authority, 2024.
- [77] VAN SCHEWICK, B. Towards an Economic Framework for Network Neutrality Regulation, Oct. 2005.
- [78] VAN SCHEWICK, B. Network Neutrality and Quality of Service: What a Non-Discrimination Rule Should Look Like. *Stanford Law Review* (June 2014).
- [79] WEBKIT. A fast, open source web browser engine. Permalink: <https://perma.cc/6FXU-98GZ>, URL: webkit.org, 2025.
- [80] WEISER, P. Regulating Interoperability: Lessons from AT&T, Microsoft, and Beyond. *Antitrust Law Journal* (Jan. 2009).
- [81] WHITTEN, A., AND TYGAR, J. D. Why Johnny can't encrypt: A usability evaluation of PGP 5.0. In *8th USENIX Security Symposium (USENIX Security 99)* (Washington, D.C., Aug. 1999).
- [82] WU, T. Network Neutrality, Broadband Discrimination. *J. on Telecomm. & High Tech. L.* 2 (Jan. 2003), 141.
- [83] WU, T., AND YOO, C. Keeping the Internet Neutral?: Tim Wu and Christopher Yoo Debate. *Federal Communications Law Journal* 59 (2007).
- [84] YOO, C. S. Beyond network neutrality. *Harvard Journal of Law & Technology* (2005).

Appendix

Fee calculations comparing App Store Fee and CTF

We briefly illustrate that the cost of paying the core technology fee (CTF) is not necessarily less expensive than the current 30% commission fee. Suppose there is an app that costs €1 and has no in-app purchases available. If this app sees 6 million downloads in one year, then the fee paid to Apple would be $6 \cdot 0.3 = 1.8$ million euros if it were distributed by the App Store, but would pay $(6 - 1) \cdot 0.5 = 2.5$ million euros if it were distributed separately and paid the CTF (which is free for the first million downloads) [22]. This constitutes a loss for the developer already in the first year. If they were to then update the app, which would be freely available to the users, after one year, they would have to pay another €2.5 million while reaping no income.

Apple also has specific requirements of the developers themselves that must be met for Apple to allow direct web distribution. Web distribution, i.e. enabling users to directly download apps from the developer's website, is a simple way for developers to have direct access to their users. In order for a developer to be granted permission to do web distribution Apple requires that developers be members of Apple Developer Program for at least two years and have an app that had more than one million first annual installs in the previous year [14]. This would prevent new developers from offering their first apps in this manner. Presumably, developers that have recently had an app with at least one million first annual installs are likely to follow-up with a similarly popular app. As with all alternative distributions, the new app would incur the CTF for all installs above one million. Apple has some exceptions to their fees for small developers and NGOs [22], but these groups are less likely to fulfill the eligibility requirements. Thus, while these requirements are ostensibly to control for responsible app developers, they track closely with criteria for selecting only those developers who will also have to pay substantial fees.

	Engineering	Vetting	Hybrid
1. How do interoperation and economic incentives clash (or not)?	Network effects are more important than interoperation and Apple can use its green bubbles to push iPhone uptake	Forcing third parties through existing vetting means collecting fees opening that up could result in a loss of revenue	Preventing interoperation keeps other developers from offering products with those functionalities
2. How do security arguments and economic incentives align (or not)?	Interoperation could reduce uptake pressure and would be an engineering challenge	Being gatekeeper on security grounds coincides with extracting rent and keeping out competition	If only in-house products can be trusted with certain features, no competitors can offer similar products
3. What needs to change in order for the company to interoperate?	Building a system that allows for interoperation and/or moving to a standard protocol	Continuing existing vetting and developing vetting for newly opened avenues, changing pricing schemes	Building in interoperation functionality as well as vetting potential new comers
4. What tension exists between security and other goals both before/after?	No tension if you do it right! Getting the whole community involved might make a more secure product	Already allowing some less than perfect actors on the platform; new system could see a loss of revenue and less security if standards are lessened	Already using a vulnerable system; interoperation could improve security or keep it the same if engineering is done well

TABLE 3. SUMMARY OF ANALYSIS RESULTS

Policy Area	Legal Case	Technology	SvI Concern Type
DMA	DMA.100097 Meta - Messenger	E2EE Messaging	Engineering
DMA	DMA.100206 Apple - new business terms	App Distribution and IAP	Vetting
		Alternative App Stores	
		Webkit	
DMA	DMA.100204 Apple - Physical Devices	OS and Physcial Devices	Hybrid
DMA	DMA.100204 Apple - Process		
Merger	M.9660 Google / Fitbit		
Antitrust	AT.40452 Apple - Mobile payments	NFC	
Merger	M.8306 Qualcomm / NXP Semiconductors		
Antitrust	AT.37792 Microsoft	Windows OS	No - Degrade
Merger	M.8314 Broadcom / Brocade	Fiber Channel SAN Switch	
Merger	M.3998 Axalto / Gemplus	SIM chips	No - Disclose
Merger	M.5669 Cisco / Tandberg	Telepresence Interoperability Protocol	
Merger	M.5984 Intel / McAfee	Malware detection	No - Both
Merger	M.6564 ARM / Giesecke & Devrient / Gemalto / JV	Trusted Execution Environment	
Merger	M.10806 Broadcom / VMware	Hardware + Software for virtualization	

TABLE 4. METHODOLOGY RESULTS