

MISGUIDED APP MARKET BILL MIRRORS EUROPE'S MISTAKES — WON'T BOOST COMPETITION, OR DECREASE COSTS.

Congress is apparently considering the App Store Freedom Act (AFSA) which copies key aspects of [Europe's failed Digital Markets Act \(DMA\)](#) – and undermines core consumer safeguards designed to protect user privacy, safety, and security. Some are now making the argument that that the legislation will save consumers money – but these claims don't match the reality of what we have seen from similar proposals in Europe.

The App Store Freedom Act would allow for unsafe alternative app stores that have as much as 50 times more malware and opens up risky payment options that do not have the basic protection necessary to protect users against malicious actors. They also require key smartphone security safeguards to be disabled in order to allow other third parties unprotected access to core features like the content of private notifications, near unrestrained access to almost everything on your phone, and access to almost anything a bad actor might want.

These regulatory proposals would mandate the inclusion of unverified alternative marketplaces—which are frequently **50 times more likely** to harbor malware—and facilitate insecure payment mechanisms that lack the basic defenses required to shield consumers from fraudulent actors. Furthermore, they require the deactivation of critical mobile security features to grant third parties unvetted access to sensitive functionality, including private notification content and nearly unrestricted entry into the device's most personal data, effectively providing a roadmap for malicious exploitation.

EUROPE'S DMA DID NOT HAVE THE INTENDED ECONOMIC EFFECTS — NOR WILL AFSA

Europe's DMA provides key lessons for how economic regulation aimed at re-architecting the technology marketplace did not have supposed positive effects. For example, one of the expected benefits of the DMA was around reduced commissions on app stores. But the actual market effects have been underwhelming. The European Commission believed that if developers pay reduced fees, those savings will be passed on to consumers through lower

prices. But a [study by Analysis Group](#) suggests that lower commission fees have not led to lower app store prices. The study looked at 41 million app store transactions across 21,000 paid apps and in-app purchases, comparing app prices for three months before developers enrolled in the alternative business terms to prices for three months after they enrolled. Ninety-one percent of the time, prices did not go down, even though fees dropped by 10 percentage points on average. In some cases, developers raised their prices. As [reported](#):

"The top five EU app developers did not change their app pricing despite the reduced commission, instead keeping the additional revenue. Developers paid an estimated 20.1 million euros less in commission fees to Apple after the change. More than 86 percent of the savings went to developers outside of the European Union.

"When developers did lower prices, the average decrease was 2.5 percent, seemingly unrelated to the DMA. Apple says that it saw the same effect when it launched the App Store Small Business Program. The lowered fees did not result in meaningful savings for consumers because only a small minority of developers decreased their prices.

"The study says that the percentage of fee reductions does not change over a longer eight-month period, and that the Core Technology Fee paid by apps with more than one million first-time installs per year also does not change the results. 80 percent of the apps in the study did not pay the CTF."

By contrast, commissions can finance platform investments that benefit both users and developers. These fees help support security, user experience, and anti-fraud protections that help foster the trust necessary for users to rely on the platform, thereby expanding the potential audience for developers. In this way, it helps strengthen consumer benefits, spurring the use of innovative apps and services as they come on-line. as.

INSTEAD OF BOOSTING COMPETITION, THE DMA IS TRIGGERING MAJOR ECONOMIC LOSSES.

One of the fundamental flaws in the DMA's framework is that rather than targeting demonstrable anticompetitive effects and cognizable consumer harms, the DMA instead [targets companies](#) based on artificial user and revenue thresholds.

Despite the DMA's stated pro-competition goals, the DMA triggered major economic [losses of as much as €114 billion for firms across the broader EU economy](#), with total turnover in the sectors considered down up to 0.64% per year since May 2023, according to economic analysis by Lama Economic Research. The study further estimates annual revenue losses per worker up to €1,122 depending on the intensity of digital service use across sectors.

Although the DMA is largely targeted at US companies, the Center for Strategic and International Studies [estimates](#) that the DMA and its companion Digital Services Act could increase costs on European businesses by as much as €71 billion per year — of which nearly half would be incurred by Europe's small and medium-sized businesses.

Likewise, an analysis by Strand Partners revealed that EU businesses estimate that [40% of their tech resources are spent on compliance with regulation](#) and that figure goes up to 45% for startups. Imagine almost half of the technology spending on the precious resources at the heart of innovation are instead being spent on compliance with regulations. These are the core barriers that Europe needs to solve to make its app ecosystem more competitive and dynamic.

According to a Nextrade Group survey of 5,000 European consumers on [the DMA's effects on Europeans' daily lives](#), two-thirds of Europeans use at least three digital services in the DMA's scope on a daily basis. But at the same time, majorities of EU consumers report new complications of using the Internet that are traceable to the DMA, for example, going directly to apps rather than having an app choice screen on their phones (59 percent.) **Majorities of Europeans, and over 70 percent in Southern Europe, would like to restore pre-DMA services.** And they would even be willing to pay a premium to get them back.

So you have regulations driving away the investment that the EU badly needs and choking the growth of its most promising scaleups.

By focusing on platform size to re-architect the technology marketplace, and ignoring any evidence of anti-competitive effects or cognizable consumer harm,, the DMA has:

1. **IGNORED** the important economic and consumer benefits from the already dynamic and vibrant smartphone marketplace and the broader app ecosystem it enables.
2. **OVERLOOKED** the many ways that the DMA makes it harder for small developers to create new apps, to reach global markets at scale in a more balkanized app marketplace, and the elevated effort now required to prevent their good ideas from being copied by others.
3. **DISREGARDED** the important and vital role that trust plays as a differentiator in enabling competition. By undermining the privacy, safety, and security that differentiated mobile platform competition has depended upon, the DMA has degraded a critical form of competition. For decades, policymakers have encouraged technology providers to compete based on who has the better privacy, security and safety safeguards as a way to drive innovation and investment – and they have - until the DMA's mandatory insecurity, and privacy walk backs stifle the ability to differentiate and compete based on metrics of trust.
4. **FAILED** to anticipate how a resultant tech gap (led by an AI tech gap) is now leaving European consumers and innovators behind, less able to incorporate AI into apps, or compete with global counterparts.
5. **OMITTED** analysis for how the DMA's mandatory mobile security weaknesses places additional burdens on Europe's brick and mortar companies that depend upon technology to run their business – forcing higher costs to defend their security and reducing their ability to compete globally.
6. **AND IGNORED** the often more essential policies that enable vibrant, innovative, safe, and secure and dynamic competition on digital platforms.

A How Distorted App Market Regulations Make it Harder for Small App Developers to Enter, Compete and Win in the Global App Marketplace

One of the stated goals of the DMA was to foster new competition. Proponents say it does so by enabling developers to use alternative app marketplaces, to link-out to alternative payment systems, and through new interoperability options. However, except for a handful of already successful developers, the DMA is making it [harder for developers](#) to create new apps, reach global markets at scale, and to prevent their good ideas from being copied by others.

An unanticipated result of this regulation has been to fracture the app marketplace ecosystem, which made it harder for Europe's small developers to gain access to the same market reach across the entirety of the global app ecosystem. While apps used to be able to get approval in one marketplace to reach global audiences, European apps must now evaluate whether to validate and invest resources in untrusted alternative marketplaces. Small developers often lack the time, money, and resources to create multiple versions of their products and undergo the multiple reviews necessary to reach every European user's default marketplace when there are as many as [300 alternative mobile app marketplaces](#). A splintered digital marketplace leaves European app developers with fewer potential customers and less market reach and higher costs to reach users. The likely result is reduced investment into developing new, more innovative, and better apps in Europe.

For years, thanks to platforms like Google Play and the Apple App Store, it's been incredibly easy for small app developers to launch a successful app and instantaneously reach global audiences. The app platforms provide the tools developers need to build, maintain, troubleshoot, market, and sell their apps to customers worldwide. [For as little as \\$25](#), they can create a developer account, access powerful software coding tools and SDKs that allow apps to be made faster than ever before, take advantage of more than 250,000 pre-built APIs to reach powerful smartphone capabilities, and get their app in front of millions of potential customers in just a few days.

Instantaneous access to global markets versus balkanized distribution. The DMA now creates new impediments and hurdles that can slow developers down, and impede their global reach. In Europe, customers can make an alternative marketplace their primary app marketplace. For app developers that means just to reach the same number of customers they previously did, instead of building two versions of their apps to sell on two trusted app marketplace platforms, they now have to build multiple versions of the app for the multiple app marketplaces within Europe – each with their own coding and technical requirements, review processes, and terms of service. And because each requires different coding for different rules, it increases the risk of coding errors, and consumes more developer resources.

A more fractured app marketplace makes it harder for apps to compete. While apps used to be able to get approval once, and reach global audiences, now apps are facing multiple global jurisdictions and DMA-like regulatory frameworks around the globe that

increase the cost of compliance, and limit their market reach. Small developers often lack the time, money, resources or ability to hire the additional developers needed to create the multiple versions of their products necessary to maintain the reach they would have had pre-DMA, to be included in all of the app stores that can become a user's default, to be able to reach the additional region specific markets that the contagion of DMA like laws are creating.

Taken together, the DMA's requirements create a more fractured app distribution marketplace that can overwhelm small, innovative app developers, [making it even harder for these small app developers to compete with larger foreign software companies](#). They now must face a DMA created balkanized app distribution marketplace that leaves them with less market reach, fewer customers, and likely lead to less focus and investment in developing new, more innovative, and better apps. Europe could and should instead be promoting policies that enable its app developers to create high-quality apps to seamlessly reach global marketplaces, via trustworthy platforms with robust app marketplace governance procedures in place that are focused on protecting consumers.

The most effective way to increase competition, sales and reach of European's most innovative home grown apps is not to adopt restrictive rules that have the effect of increasing developer costs, compliance burdens, fail to bring benefit to consumers, and disincentivize platforms from driving innovation in the EU. Creating a fractured app marketplace and restricting an app's reach, and thus its market potential, does not boost Europe's competitiveness, and isn't fair to developers. A better approach promotes smart and sensible rules that enable Europeans apps to reach global markets on trustworthy platforms so they can compete globally, and capture global share.

B Differentiation enables mobile platform competition.

One of the key ways regulators can enable greater competition between platforms is to enable, not squelch, greater smartphone market differentiation. It means giving companies the breathing room they need to offer unique features that set them apart from each other in a very competitive market, rather than [forcing them to become more alike](#). Intra-platform mobile competition has been a key driver of consumer benefits. Apple and Google engage in direct and sustained competition across their entire mobile ecosystems -- spanning devices, browsers, and app stores.

Many consumers specifically choose Apple devices because of their features, and their integrated, secure ecosystem. Others specifically choose Android because of its features, and more open approach. This differentiation enables dynamic market competition where companies invest in new technology, drive innovation, improve trustworthiness, to enable consumers to do new things, enable apps on their platforms to become more feature rich, and allow consumers to make market choices about which is the best technology that meets their needs. It enables companies to offer different value propositions, and business models, to meet different consumer and business preferences. But the DMA has substantially weakened

this competitive environment and eliminated key consumer choices by forcing all platforms to operate under the same government-mandated rules – making both platforms operate more in the same way, decreasing the core differentiation that has driven competition.

The DMA and AFSA, however, are premised on a faulty belief that governments cannot trust consumers to freely decide in the market for themselves which platform provides the most value, which platform is the most trustworthy, and which platform has integrated technologies that best meet their needs. That's what a competitive digital market looks like – differentiation built on innovation, price, features, and indeed trust. But lowering trust, and taking away key features used in the market to differentiate a product, does not foster more competition, it just limits choices. Rather than trusting consumers to make their own market choices and empowering users with better information and options to make those choices with, it is forcing companies to make their products with less differentiation with the belief that the government is in a better position to make choices for how to shape digital markets and limit the differentiation that consumer can choose.

C Traditional Businesses are put at competitive disadvantage globally because of mandated security weaknesses.

The DMA has features that mandate insecurity which doesn't enable competition or make markets fairer. It creates significant new security threats to enterprise networks, critical infrastructure, and daily operations - at a time of global cyber conflict. If enterprise customers are less secure, they will face the risk of, and are more likely to experience, actual damage - stolen intellectual property, ransomed data, transfer of cash, theft of customer and partner data, and loss of production operations. If enterprises can not escape the effects of these government imposed higher vulnerabilities, they face higher remediation costs responding to their losses. And even if they escape the higher likelihood of exploitation, they will have to prepare for the increased risk and invest significantly more to defend against threats that their global competitors are better protected from, and be less competitive in global markets. For example, a single mobile malware exploit could cost businesses hundreds of millions.

- **As the DMA weakens phishing safeguards, experts report that a single mobile phishing attack** could [cost a 5,000-employee organization almost \\$4 million](#) according to Lookout. But unmitigated mobile phishing threats could end up [costing organizations with 10,000 mobile devices as much as \\$35 million per incident](#) and up to [\\$150 million per incident](#) for organizations with 50,000 mobile devices. This comes at a time when Zimperium found that [82% of all phishing sites](#) now target mobile devices, and Lookout's threat report found that [mobile phishing is now one of the biggest challenges facing IT and security teams today.](#)
- **SMEs are particularly at risk.** For small and medium businesses, the average cost of a cyber-attack [range between \\$120,000 and \\$150,000](#), with some breaches potentially costing much more depending on the severity, company size and industry. New DMA

mandated security weaknesses, and increased risks will put these SMEs at a further competitive disadvantage globally.

- **A single ransomware attack** costs companies [\\$5.08 million](#) on average according to IBM's 2025 Cost of a Data Breach Report. The average cost of a single data breach is \$4.4 million, according to IBM. Add on top of that the non-compliance costs following a breach which can cost a company up to 4% of annual global turnover in GDPR fines.

And because smartphones are in the pockets and purses of almost every CEO, critical infrastructure operator, national security professional, elected official, military commander, judge, and journalist, when weakening security for one, it weakens it for us all.

D Europeans Want To Restore Pre-DMA Opportunity

Majorities of Europeans, and over 70 percent in Southern Europe, [would like to restore pre-DMA services](#), and they would even be willing to pay a premium to get them back – according to a survey of 5,000 European consumers on the DMA's effects on Europeans' daily lives. For example, 55 percent of higher-income and 52 percent of lower-income consumers would be willing to pay more to restore pre-DMA technology to ensure safe payments for gatekeeper operated app marketplaces – the number one priority for higher earners in the survey. It shows consumers assign clear and often significant values to the trusted app payment systems provided by gatekeepers, moored by the very safeguards that DMA regulators have sought to weaken.

TO BUILD TRUST, we need to raise not lower cybersecurity protections, improve privacy protection not weaken them, and boost digital safeguards instead of opening the door to a vast array of new scams and frauds.

Thus, this is not the time to recycle or to adopt Europe's failed experiments, to push through legislation that we know has deep flaws or to rush an effort that has not been fully baked. Instead of inadvertently taking steps backwards, we urge leaders to stay the course by continuing to press forward on advancing pragmatic policies and private sector action on efforts to improve privacy, safety, security, and trust in our digital ecosystem. **Because continued advances that drive continuously better privacy, safety and security are the keys to enabling a more trusted future.**