TRUSTED FUTURE

FAILED EXPERIMENT: THE DIGITAL MARKETS ACT'S VAST UNINTENDED CONSEQUENCES

CONTRADICTIONS IN THE EU'S DIGITAL GOVERNANCE FRAMEWORK CREATE POTENTIALLY CATASTROPHIC CONSEQUENCES — AND REQUIRE IMMEDIATE PATCHING AND A REBOOT

By Jim Kohlenberger | Co-chair of Trusted Future

October 2025
Failed Experiment
Report 1_4

As the European Union enforces its Digital Markets Act (DMA), it is raising fundamental questions about Europe's approach to digital markets regulation, how it may actually be undermining Europe's long-term ability to improve its digital ecosystem, and unintentionally exposing Europeans to new harms, without any commensurate ability to move swiftly to fix things. This report series assesses the unintended effects of the DMA and finds that contradictions in the EU's digital governance framework create potentially catastrophic consequences – and require immediate patching and a reboot.

Though the DMA aims to promote competition in Europe's digital ecosystem, this report series explores three foundational mistakes with long-last impacts:

↗ CREATING AN APP GOVERNANCE GAP:

The digital disconnect between the EU's Digital Services Act's (DSA) ambitions for a safer app store ecosystem and the DMA's disjointed digital agenda that expands some of the exact harms the DSA tries to mitigate.

↗ DAMAGING MOBILE SECURITY:

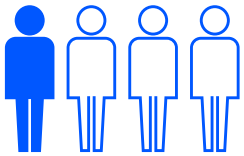
The many ways the DMA weakens security and the near-catastrophic consequences it could bring to Europe's consumers, businesses, critical infrastructure, and national security.

↗ IMPEDING COMPETITION AND HINDERING POTENTIAL:

The DMA's impact on Europe's broader economic ecosystem, including ways it actually inhibits competition and opportunities to advance a more dynamic, vibrant, innovative, and trustworthy ecosystem that can lift its economy and propel new competition.

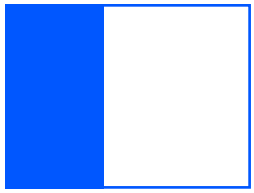
These consequences have real-world impacts for consumers and businesses:

1. Consumers face increased security risks, at a time when digital frauds and scams already impact



1 in 4
Europeans every year.

2. Businesses face an unfriendly regulatory environment, with



European companies spending
40%
of their tech resources on compliance with regulation.

3. European markets are left with less innovation, fewer and delayed features, and — ironically — less consumer choice.

This first installment of the series also examines a series of case studies of how these regulatory impacts play out in person.

- → Protecting children from illicit and pornographic content
- → Establishing effective platform-level parental control tools
- → Protecting children's privacy and security by default
- → Protecting intellectual property
- → Protecting consumers from frauds and scams
- → Protecting democratic processes and election integrity
- → Protecting women from online gender-based violence

Europeans deserve a vibrant mobile digital ecosystem that is innovative, safe and secure, competitive and trustworthy. Europe's policymakers have taken important steps towards a better digital ecosystem but the DMA threatens this forward progress. This regulation is driving Europe backwards towards a potentially disastrous digital danger zone. Today, as a result of the DMA's implementation, European consumers and businesses face a less secure, less innovative, and more fragmented digital experience.

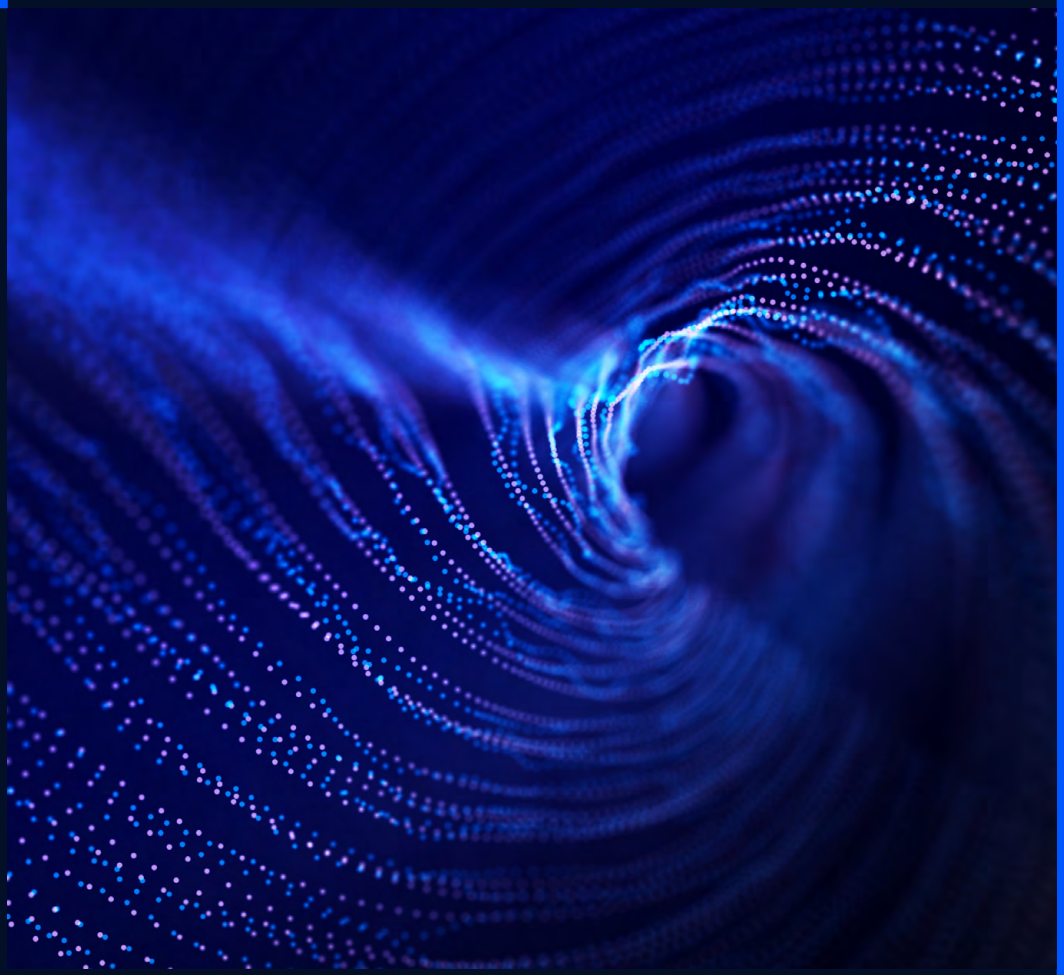
While Europe has rightfully criticized Silicon Valley for its "move fast and break things" approach to technology, Europe's DMA risks taking the same approach in its regulations for consumer facing technology. This is a bad technology development approach and an even worse regulatory approach. As the DMA is enacted, it is raising fundamental questions about Europe's approach to digital markets regulation, how it may actually be undermining Europe's long-term ability to improve its digital ecosystem, and unintentionally exposing Europeans to new harms, without any commensurate ability to move swiftly to fix things.

This timely report includes recommendations for policymakers in Europe to address the fundamental flaws of these regulations, and **a warning for regulators around the world who may be looking to copy the EU's example**. With over 70% of Southern Europeans preferring to restore pre-DMA services, the DMA is a failed experiment that must be remedied and not replicated.

Over 70%

of people in Southern Europe say they would prefer to **restore pre-DMA services**

TRUSTED FUTURE



APP GOVERNANCE GAP:

THE HIGH COST OF THE DSA VS. DMA DISCONNECT

October 2025

Failed Experiment

Report 1_4

APP GOVERNANCE GAP: THE HIGH COST OF THE DSA VS. DMA DISCONNECT

Europe's Digital Services Act includes provisions designed to make app stores safer. The Digital Markets Act aims to make markets more competitive. While these regulations were conceived in unison, for mobile devices, their goals and mandates are fundamentally at odds with each other.

The Digital Services Act has its own set of implementation flaws which are not covered here. Instead, we use the DSA's laudable policy goals of improving and advancing a more trustworthy digital ecosystem as a measuring stick by which to measure the effects of the Digital Markets Act.

As Margrethe Vestager has explained in describing the differences between the two statutes, the DMA, "forces dominant players to open the gates of the market." By contrast, DSA essentially requires the same very large platforms to "man the gates" more thoroughly by taking risk-based actions to restrict the types of content that comes through the gate and onto their platforms.

So while the DSA obligations are designed to ensure that platform gateways are appropriately guarded and monitored, the DMA goes in the opposite direction by requiring that gateways be opened up, creating unguarded side doors and unregulated back doors that let bad actors exploit Europeans' trust. Put another way, while the DSA sees enhanced gatekeeping as the solution, the DMA sees gatekeeping as the problem and as a result it weakens a platform's safeguards aimed at protecting users.

APP GOVERNANCE BEFORE AND AFTER THE DMA AND DSA'S INTERVENTIONS

Prior to the existence of these two new laws, smartphone manufacturers spent years developing, improving and vigorously enforcing a robust app governance framework. Under these policies, platforms reviewed and governed the safety, security, privacy, and trustworthiness of mobile app ecosystems. These governance mechanisms in turn helped enable the vibrantly competitive app ecosystem whereby apps all play by the same set of basic safeguards and consumer protections. By meticulously reviewing apps before they made their way to the marketplace, these governance systems prevented billions in frauds and scams, privacy abuses, malware threats, and intellectual property theft. They have also proven to be essential for detecting security vulnerabilities before they cause harm to businesses or user privacy. These platforms have fortified this approach with a comprehensive set of built-in parental controls to protect children from a variety of online harms that could stem from apps.

These app governance systems were designed to create and enforce commonsense guardrails and limit harmful content that the DSA now wants to ensure are restricted on mobile platforms. The DSA's regulators applied its rules to the two primary mobile app marketplaces, building upon existing app governance systems. Among other things, these DSA rules seek to limit access to harmful and illegal content, bolster consumer protections against fraud and scams, protect minors from illicit content, and better protect intellectual property in its regulated app marketplaces.

However, by contrast, the DMA specifically prohibits the same regulated entities from restricting access to the exact same kinds of harmful content across the entirety of their platform. The DMA is thus creating new backdoors and ways to get around the pre-existing and proven app governance systems without replacing it with any kind of new app governance system.

> THE DMA IS CREATING NEW BACKDOORS AND WAYS TO GET AROUND THE PRE-EXISTING AND PROVEN APP GOVERNANCE SYSTEMS WITHOUT REPLACING IT WITH ANY KIND OF NEW APP GOVERNANCE SYSTEM.

As a result, the DMA has unintentionally created a gaping app governance gap with potentially catastrophic consequences for European innovators, businesses, and consumers. By forcing gatekeepers to change their app governance policies, and inhibiting the normal app review process, the DMA is breaking key safeguards meant to protect consumer safety, security, and privacy. The app governance system built by the smartphone manufacturers aims to protect consumers from frauds and scams, to protect against intellectual property theft, to provide parents with tools to protect children, and to enable innovators to quickly and seamlessly gain access to a trusted mobile ecosystem with near global reach. While the DSA seeks to bolster these gatekeeper protections, the DMA undoes these protections by fundamentally breaking the comprehensive governance model without replacing it with another mechanism. The result is dismantled consumer protections with significant negative long-term impacts on users.

In examining the digital disconnect between the DSA and DMA, it is unlikely that regulators anticipated the practical consequences of opening up the gatekeepers' gates. The case studies reviewed below, demonstrate how the DMA has opened the floodgates to apps with illicit and pornographic content; allowed innovative new ways to defraud, scam, and rip off consumers and businesses; created a rush in intellectual property theft enabling apps; expanded Russian abilities to launch disinformation campaigns; and opened a backdoor through which parents can no longer protect children and the apps they access.

THE IMPACTS OF THE GOVERNANCE GAP

Fundamentally, this governance gap means that an app taken down or blocked under the DSA, can now get around these restrictions by getting sideloaded straight back onto the platform under DMA mandates. In practice, the DSA's goals of protecting kids, creators, or consumers are inherently incompatible with how the DMA is being implemented.

Compounding these effects, the DMA also requires that users be able to download largely ungoverned alternative app marketplaces and even requires the ability to make them their smartphone's default app marketplace. Alternative app marketplaces are notoriously unsafe and scammy, with some carrying more than 60,000 malicious apps in a single year. They are ill-equipped to fill the governance gap, and don't have any obligations under either the DMA, or the DSA. For example, alternative app marketplaces aren't even contemplated by the DSA. They have zero obligations to address any of the critical harms outlined by Article 34 of the DSA, and no obligation to expeditiously remove harmful content when notified by a trusted flagger.

> THIS GOVERNANCE GAP MEANS THAT AN APP TAKEN DOWN OR BLOCKED UNDER THE DSA CAN NOW GET AROUND THESE RESTRICTIONS BY GETTING SIDELOADED STRAIGHT BACK ONTO THE PLATFORM UNDER DMA MANDATES.

↗ THE MAGNITUDE OF THIS SIDELOADING SIDE EFFECT

Between October 2023 and February 2025, Trusted Future analyzed 59,767 apps removed from Apple's App Store under the DSA's transparency filings. 98.7% of these apps, many removed for nefarious or harmful content, are able to get right back on European devices because of DMA loopholes that allow apps to bypass trusted review systems.

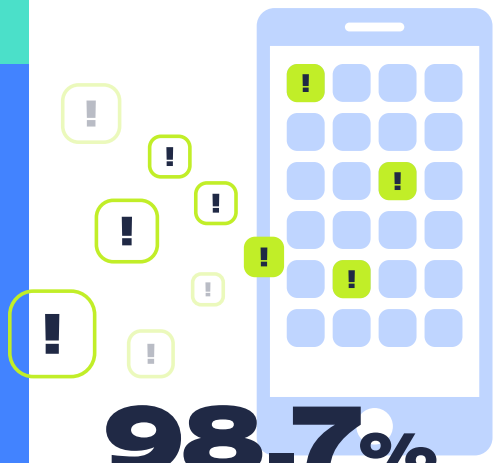
THE GAP

↗ THE DSA

The Digital Services Act was ***designed to keep harmful content off European devices.***

↗ THE DMA

The Digital Markets Act ***creates a sideloading loophole that opens devices to harmful apps.***



98.7%

of apps taken down from Apple's App Store for harmful content could get right back on European devices because of the DMA's flaws.

THE RESULT:

A BACKDOOR FOR HARMFUL APPS

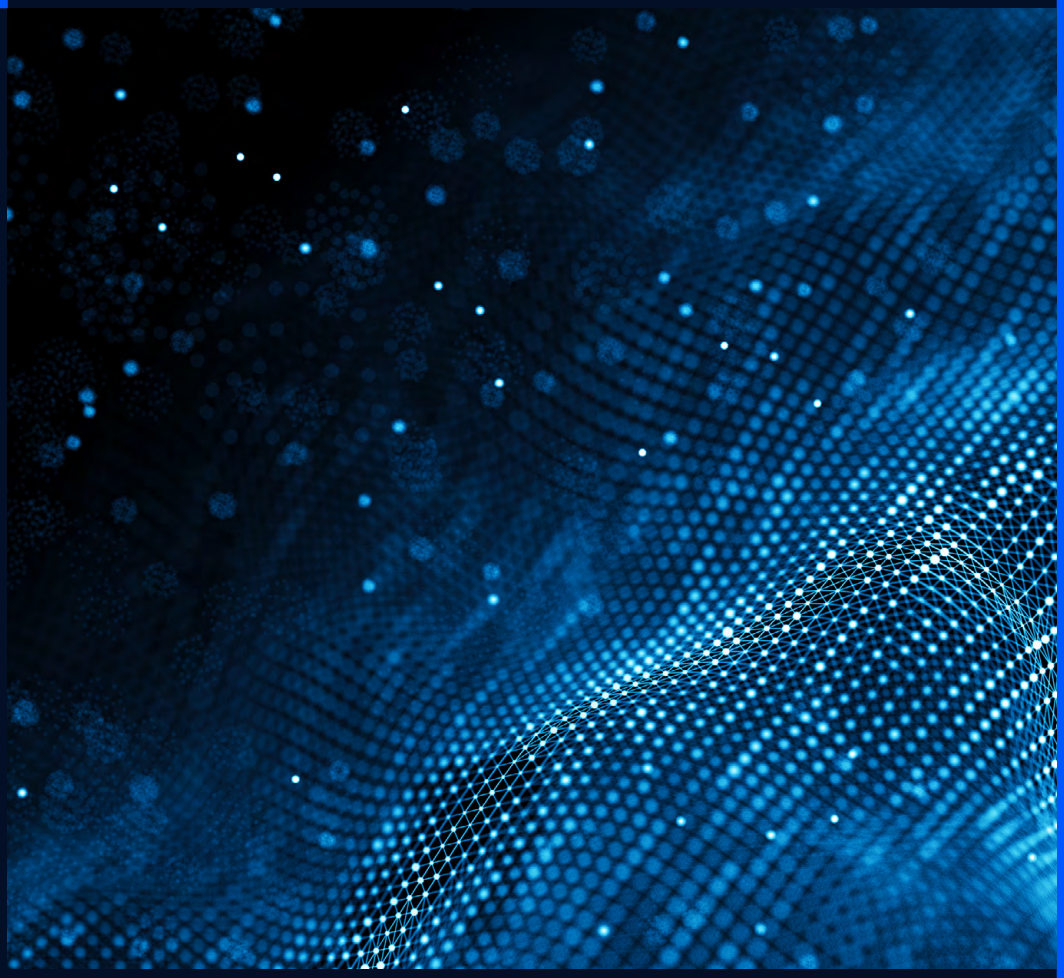
As a result, tens of thousands of unsafe apps now have a backdoor to return to users' phones via:

- ↗ ***Direct web downloads (sideloading)***
- ↗ ***Unregulated alternative app marketplaces***

Without DSA-level transparency or oversight, policymakers have no visibility into whether third-party app stores let harmful blocked apps back on or spread new risks across the EU.

> THESE TENS OF THOUSANDS OF HARMFUL APPS BLOCKED FOR CONTENT REASONS (PER THE DSA) NOW HAVE A BIG BACKDOOR TO GET BACK ONTO THE PLATFORM VIA DIRECT WEB DOWNLOADS (SIDELOADING) OR THROUGH AN ALTERNATIVE APP MARKETPLACE AS PART OF THE GOVERNANCE GAP CREATED BY THE DMA.

TRUSTED FUTURE



CASE STUDIES

EXAMINING THE DISCONNECT BETWEEN THE DSA AND DMA THROUGH SIDELOADING SIDE EFFECTS

This series of case studies looks closely at the digital disconnect between the DSA's broad regulatory goals for app marketplaces, the effectiveness of existing official app governance systems, and explores more specifically the very real harms that, despite wellmeaning intent, the DMA is delivering to European consumers.

October 2025
Failed Experiment
Report 1_4

CASE STUDIES

1↗ PROTECTING CHILDREN FROM ILLICIT & PORNOGRAPHIC CONTENT

BEFORE THE DMA

Today's children are the most connected generation in history, but also some of the most vulnerable users of new technologies. Given the breadth and depth of potential online harms and vulnerabilities, both app governance systems and the DSA's authors have made safeguarding minors a primary objective. For example, Apple's App Store has long rejected illicit and pornographic apps through its terms of service. Google's Play Store likewise prevents apps containing or promoting pornography. Building on these app governance mechanisms aimed at protecting kids, EC regulators outlined stringent and specific steps that the two primary app marketplaces must take to meet the DSA requirements that they "design their services ... to address and prevent risks to the well-being of children ... and prevent minors from accessing pornographic content online."

AFTER THE DMA

By contrast, DMA mandates now require that iPhones give European users expanded access to pornographic, illicit, and related adult apps through third party app stores – including new hard-core pornographic distribution apps -- and do so in a way that gets around built-in device level parental controls. This DMA-created digital disconnect happens because the DMA prohibits device producers from restricting apps for content purposes that are made available outside of official app marketplaces. The DSA's efforts to restrict this same pornographic content has been thwarted by the DMA-created governance gap.

2↗ ESTABLISHING EFFECTIVE PLATFORM LEVEL PARENTAL CONTROL TOOLS

BEFORE THE DMA

Article 34 of the DSA requires the two primary app marketplaces to establish and maintain effective parental control tools. Prior to DMA implementation, a parent could utilize and rely on a broad range of platform-level app marketplace enabled tools to, for example, enable easy access to every app's age rating on an app store download page, prevent children from buying or downloading apps onto their phones without parental approval, and to block mature content.

AFTER THE DMA

Because of the DMA, none of these tools are now universally available across the entirety of the platform. That means that parents can't ensure that their children are appropriately protected. Now in the EU, and the EU only, these simple platform-based parental controls are far more complicated, and completely unavailable for apps downloaded directly onto phones, or via alternative app marketplaces. Parents in Europe are unlikely to be aware that they may no longer be able to rely on the tools built into official app marketplaces to comprehensively protect their children across the platform – like the app store age rating system, "Ask to Buy" tool, or limits on mature content. These and other important, popular, and DSA-required parental control tools have been thwarted by the DMA created governance gap.

3↗ PROTECTING CHILDREN'S PRIVACY & SECURITY BY DEFAULT

BEFORE THE DMA

Notifications are an integral part of the way children communicate and use smartphones, helping them stay informed about messages, calls, weather alerts, events on their calendar, and more at a glance. Children's privacy protection has long been a core priority of smartphone providers, and the DSA backed that up by requiring the two primary app marketplaces to protect minors by "adopting special privacy and security settings by default," including for things like notifications.

AFTER THE DMA

Because of poorly thought through DMA mandates, those same notifications can be intercepted and used to put children's private data at risk. The DMA's interoperability requirements (Article 6.7) have been applied to Apple – and only Apple – in a way that undermines key privacy protections by default. For example, DMA rules require Apple to provide third-party devices the content of all smartphone notifications – giving data- hungry apps the opportunity to hoover up all of a child's personal and private notifications in an unencrypted form to be sent to its servers – where it could be mined, used for targeted ads to underage minors, or sold to unscrupulous third parties without restriction. Critical DSA-enabled children's privacy and mobile phone privacy safeguards that keep sensitive information encrypted, protected, and secure are being weakened and thwarted by the DMA's unwise interoperability mandates.

4↗ PROTECTING INTELLECTUAL PROPERTY

BEFORE THE DMA

The DSA seeks to combat counterfeiting and to better protect intellectual property, and to enable "urgent action from providers ... to minimize the harm caused by illegal streaming." The DSA created a "Trusted Flagger" system that allows content owners to flag copyright and intellectual property infringements, which the two primary app marketplaces are then required to act expeditiously to address. In conjunction, the two primary app marketplaces have worked diligently to prevent piracy, intellectual property theft, and illegal streaming on their platforms by blocking and taking down problematic apps.

AFTER THE DMA

Because alternative app marketplaces don't have these DSA obligations, and because the DMA forbids platforms from policing apps distributed outside of official app stores for content reasons, the DMA is poised to become one of the greatest enablers of intellectual property theft in European history. Flagship DMA-enabled third-party app stores are being anchored by previously banned torrenting apps, illegal streaming apps, ROM emulators for pirating games, and counterfeit apps – which together are enabling intellectual property theft at a whole new scale and scope. The DSA and app governance mechanisms designed to protect intellectual property have now been thwarted by the DMA's gaping governance gap. This is especially harmful for Europe, where activities involving Intellectual Property constitute almost 50% of the EU GDP and provide nearly 40% of employment.

5↗ PROTECTING CONSUMERS FROM FRAUDS & SCAMS

BEFORE THE DMA

As Europe faces a surging online fraud problem impacting 1 in 4 Europeans, the DSA required the two major app stores to put in place measures to ensure a "high-level of consumer protection." This helps protect consumers from online scams, misleading advertising, illegal products, unfair practices, and the misuse of their personal data. These requirements are on top of the robust governance mechanisms these platforms use to fight fraud and scams on their platforms; both Apple and Google have prevented billions of dollars in fraudulent and abusive transactions through their app stores.

AFTER THE DMA

Europe is already facing a sideloading based "Scamdemic" that is ripping off consumers and draining bank accounts. Now, the DMA is making things worse by giving bad apps a backdoor way around consumer protections. The DMA's 5(4) obligations allow developers to link to external websites outside of a trusted app store ecosystem without privacy and security safeguards. Sideloaded apps can maliciously trick users with links used to hijack accounts or give away sensitive information via fake login pages. Consumers are less able to seek redress in the event of a scam or fraud. That's because key official app store protections can't apply to these link-out transactions. The $200 billion cryptocurrency exchange Coinbase, for example, found it necessary to warn all of its European customers that as a result of the DMA, consumers need to be aware of fraudulent Coinbase apps on iOS which could be used "to intercept your personal information, financial assets and other sensitive data."

6↗ PPROTECTING DEMOCRATIC PROCESSES & ELECTION INTEGRITY

BEFORE THE DMA

At a time when 86% of Europeans agree that the rapid spread of disinformation is a major threat to democracy, new DSA obligations for app stores prioritize the integrity of the democratic electoral process. When the EU raised concerns that Russian state-controlled media outlets RT and Sputnik were distributing disinformation related to Russia's invasion of Ukraine, Apple pulled the Russian state-owned media outlets RT and Sputnik from global app marketplaces and Google pulled it from its European app marketplace.

AFTER THE DMA

Ironically, Russia has now adopted its own DMA-like bill requiring the installation of a government-backed third party app marketplace made popular in Russia after Apple and Google removed apps. The result is that, despite the DSA's effort to thwart disinformation-spewing apps, the DMA could make RT, Sputnik, and a host of other disinformation-spewing and spying apps more available for sideloading in Europe. Politico has described this as the Kremlin putting a spy in every new phone. The alternative app stores and direct sideloading of apps also open the door to fake but legitimate looking apps mimicking official European news outlets. While the DSA's guideline 16(h) on service integrity call on official app marketplaces to put in place appropriate procedures for timely detection and disruption of activity that could impact election integrity, the DMA has taken away the app governance tools that an mobile platform would need to do so.

7↗ PROTECTING WOMEN FROM ONLINE GENDER BASED VIOLENCE

BEFORE THE DMA

The DSA gives the two primary app marketplaces obligations to assess and mitigate the risks of online gender-based violence. Cyberstalking often starts with someone surreptitiously installing an app on another person's phone to stalk their every movement, message, and intimate details — putting a stalker or domestic abuser right in their pocket or purse. As more than half (54%) of domestic abusers tracked survivors' mobile phones using stalkerware apps, according to the National Network to End Domestic Violence, official app stores have long sought to block these insidious apps.

AFTER THE DMA

Now, the ability to limit access to stalkerware and spyware apps and prevent gender-based violence have fallen into the EU's app governance gap. Spyware and Stalkerware app usage is now surging in Europe, despite the huge privacy and security concerns, and strong governance from official app stores – likely due to sideloading allowed under the DMA. Last year, security researchers identified 195 different stalkerware apps, and detected 2,645 unique cases of stalkerware in Europe. While app marketplace governance mechanisms have long sought to restrict them, and the DSA requires official app marketplaces to address these risks, these efforts are once again thwarted by the DMA's app governance gap.

These are powerful examples of how the DMA is impeding Europe's own efforts to improve the digital ecosystem and create a safer and more accountable digital ecosystem. By opening up the gatekeepers' gates, the DMA has opened the floodgates to apps with illicit and pornographic content that defraud, scam, and rip off consumers and businesses, that steal intellectual property, expand Russian disinformation campaigns, and that limit a parent's ability to protect their kids. Europeans deserve better than disjointed rules that put kids, creators, and consumers at substantial risk.

TRUSTED FUTURE

DIGITAL SECURITY DISCONNECT:

HOW THE DMA CREATES AND EXACERBATES MOBILE SECURITY RISKS

October 2025

Failed Experiment

Report 1_4

DIGITAL SECURITY DISCONNECT: HOW THE DMA CREATES AND EXACERBATES MOBILE SECURITY RISKS

Many bad actors have adopted a mobile-first attack strategy as smartphones have become more essential in our daily lives and the global economy. This makes it essential that policymakers, organizations, and users understand and take steps to mitigate mobile security risks. But the implementation of the DMA risks exacerbating and widening these security risks, at a time when businesses and users can't afford to let their guards down.

More than four billion mobile-focused social engineering attacks occurred in 2024 alone. Users recognize these threats: three-quarters of Europeans want stronger cybersecurity according to Eurobarometer. And policymakers have tried to respond: the Cyber Resilience Act (CRA) requires smartphone manufacturers to build robust security protections into the heart of their technologies from the start by design. But when it comes to the DMA, regulators have created a digital disconnect by undoing important security policy goals. Instead of working in synchrony with policies like the CRA to improve security and trust, the DMA creates vast new security weaknesses that put European consumers and businesses at risk.

The implementation of the DMA is making users less safe, in three broad ways:

1

It enables harmful and malicious apps to make unregulated end-runs around the existing successful app governance system.

2

Its interoperability rules disable key security safeguards designed to protect user privacy and safety.

3

Its anti-steering/link-out provisions create opportunities for bad actors to steal sensitive financial information, exposing Europeans to increased risks of malware, phishing, and fraud.

These DMA requirements are dangerous missteps that weaken existing security safeguards that were instrumental in protecting European businesses and consumers. It is unlikely that policymakers anticipated that when enforcing the DMA they would be requiring platforms to make foundational changes that undermine basic security best practices and erode steps towards broader European policy goals. Moreover, during implementation, the DMA's rules have not been subject to any kind of comprehensive review by European cyber or national security expert agencies, and its requirements are in direct conflict with the goals and requirements of the Cyber Resilience Act (CRA). In practice, regulations that require smartphone manufacturers to build robust security protections into the heart of their technologies from the start by design are now in conflict with the DMA's implementation.

> THE DMA NOW FORCES MASSIVE NEW SECURITY WEAKNESSES AND VULNERABILITIES INTO AN ALREADY WELL-DESIGNED SECURITY ARCHITECTURE.

The result is that the DMA now forces massive new security weaknesses and vulnerabilities into an already well-designed security architecture. This puts European consumers, businesses, and critical infrastructure providers at increased risk. There are three key DMA mandates that are creating these risks: mandated insecure interoperability requests, anti-steering and link-out permissions, and side-loading.

THE PROBLEMS WITH MANDATORY UNSECURE INTEROPERABILITY

Interoperability can be a game-changer, but unsecure interoperability can be a security nightmare. Taken together, the technology changes being enforced under the DMA represent the most extensive mandated insecurity regime in modern technology history. It is transforming Europe's mobile marketplace into a digital danger zone.

It may be one reason why Edelman's Trust Barometer for the Europe Region Report found that 59% of respondents believe government regulators lack adequate understanding of emerging technologies to regulate them effectively (including 65% in Italy, 60% in Germany, 60% in the Netherlands, 56% in France, 55% in Sweden, and 53% in Spain.) Article 6.7 of the DMA focuses on enabling new forms of competition by requiring mobile platforms to be interoperable with core hardware and software features controlled by its operating system. But under the well-meaning goal of advancing digital interoperability across many platforms, the EU has nonetheless required just one company – Apple – to disable key security safeguards, expose sensitive internal systems, and weaken core safeguards designed to protect user privacy, safety, and trust in order to allow other third parties to access core features like notification content, sensitive permissions, automatic Wi-Fi login information, and almost any other information a bad actor might want.

Because the DMA gives the European Commission (EC) flexibility and deference in implementing the law, EC staff have a free hand to dictate these intricate technology changes without regular due process and regulatory constraints. As a result, EC staff have crafted intricate interoperability rules for Apple, and Apple only, including requiring mandated access for complex technologies without taking into account even basic security practices. There are three public examples of how this has already weakened digital security: push notification privacy, sensitive permission abuse, and just-in-time computing.

PUSH NOTIFICATION PRIVACY

Push notifications – alerts that pop up on your smartphone screen – play an integral role in the way we use smartphones. They help us stay informed about messages, calls, weather alerts, events, news, multi-factor authentication codes, and a host of other private information at a glance. But they are also enormously valuable to unscrupulous third parties. Russia and other governments have long sought access to Google and Apple smartphone notifications as a way to surveil users. Hackers want access to notifications and texts because they contain temporary access codes that can be used to bypass multi-factor authentication security. Social media giants, infamous for their invasive data collection habits, want access to covertly extract unique device data to fingerprint smartphones, bypass popular protections that allow users to "Ask Apps Not To Track," and use the unique digital fingerprint to track and target users with invasive ads. None of these examples are aligned with Europe's overall policy goals.

> THESE CHANGES ENABLE THIRD-PARTY CONNECTED APPS TO INTERCEPT, STORE, AND MONITOR PERSONAL COMMUNICATIONS AT SCALE WITHOUT BASIC PROTECTIONS — SIDESTEPPING THE SECURITY AND PRIVACY PROTECTIONS BUILT INTO THE PLATFORM'S GOVERNANCE MECHANISMS.

Despite these potential harms, DMA regulators have implemented the law in a way that disregards built-in security protection and allows the third-parties to gain access to these notifications without having commensurate security and privacy

protections in place. DMA regulators have written specific notification interoperability requirements (under Article 6.7) in a way that requires Apple (and only Apple) to provide third-party devices the content of all smartphone notifications. In practice, this gives third-parties access to a broad range of sensitive and personal information that even Apple can't see without requiring the same standards that protect privacy and security. These changes enable third-party connected apps to intercept, store, and monitor personal communications at scale without basic protections — sidestepping the security and privacy protections built into the platform's governance mechanisms.

The rules also undermine the built-in security of notifications by busting open the inherent strength of end-to-end-encryption that protects notifications from being interrupted or unencrypted. Alarmed by this prospect, U.S. regulators wrote to the U.S. companies covered by the DMA to warn that "[w]eakening encryption or other security measures to comply with the laws, demands, or expected demands of a foreign government" likely violates U.S. law. It's thus not surprising that only 31% of Europeans believe that government agencies are taking sufficient measures to protect their digital identity and data.

This notification nightmare creates significant new weaknesses for business owners, critical infrastructure providers, national security officials, journalists, children, and nearly everyone else who uses a smartphone.

SENSITIVE PERMISSION ABUSE

While permissions seem innocuous at first glance, security researchers consider many permissions to be "high-risk" because they can involve broad access to your camera, microphone, locations, contacts, photos, calendars, messages, identify nearby Wi-Fi devices, read call logs, and even social media login permissions. When used together, these permissions can significantly compromise user privacy and security, enable surveillance, allow bad actors to exfiltrate sensitive corporate or personal data, facilitate behavioral tracking, and expose location data, all of which could jeopardize physical safety.

Google reports that frequently abused permissions, like enabling an app to read and send SMS messages or to access powerful accessibility features, are commonly used by fraudsters to intercept one-time passwords, spy on screen content to access login credentials, or see other sensitive and exploitable information. Based on Google's analysis, over 95 percent of installations that abuse sensitive permissions came from Internet-sideloading sources.

A CyberNews analysis found that some apps requested a broad range of permission that go far beyond the minimum amount to enable the apps to function. Apps can also access data for wide-ranging purposes, for example Meta rolled out a new feature based on access to your phone's camera roll to automatically send all of your photos to its servers, use its facial recognition software, and train its AI models. The EC's enforcement of the DMA makes these permissions even more broadly allowable, without limit.

Importantly, the EC's forced changes to permission structures are at odds with what European users want. In a Eurobarometer poll, respondents were most likely to specify the misuse of personal data (46%) as the issue that has the most personal impact in the EU's regulation of online platforms.

The consequence of this DMA enforcement could be that companies fined under the GDPR multiple times for privacy abuse – could be given the keys to expand user data exploitation in ways previously unimaginable. Here again, basic privacy protections, and technologies once thought to be secure, are falling through the DMAs mandatory governance gap.

UNSECURE INTEROPERABILITY MANDATES

Rather than using an evidence-based approach to address specific consumer harm, the DMA imposes broad brush rules that fundamentally change how technology works without any evidence that consumers want the changes or consumer benefits. Just In Time computing, or JIT, is an example of the kinds of major mobile security risks that DMA 'interoperability proponents ignore, and the kind of security weakness that DMA regulators keep building into their smartphone rules that could have severe long-term security and financial implications.

Trusted Future examined the first interoperability request publicly posted as part of the Apple specific interoperability rules and found a digital doozy that would enable vast new security threats. A developer has requested that under the DMA's new interoperability rules, Apple should provide it with direct access to the ability to directly write and execute unsigned code in memory, a feature of its Just-In-Time Compiler or JIT engine – which is a core capability built into all major browser engines.

> THE DMA IMPOSES BROAD BRUSH RULES THAT FUNDAMENTALLY CHANGE HOW TECHNOLOGY WORKS WITHOUT ANY EVIDENCE THAT CONSUMERS WANT THE CHANGES OR CONSUMER BENEFITS.

A JIT engine is the software used by web browsers to compile code from a web-based language to the language the operating system the smartphone understands. It is a crucial function that helps web browsers work faster and more efficiently.

Many experts believe a JIT engine is so critical, complex, notoriously difficult to debug, and vulnerable that it has been at the heart of roughly half of all web browser exploits across every major web browser, was involved in surreptitiously gaining broad control of smartphones in the original Pegasus mercenary spyware exploit, and Russian hackers are actively working to exploit bugs in JIT software as part of a sophisticated exploit chain to attack adversaries, plant malware and steal information. Given the serious nature of these threats, the JIT is a core feature that gets turned off when you activate Apple's "Lockdown Mode," Microsoft's "Super Duper Secure Mode," and Chrome's "Secure Mode."

Europe's DMA rules now seemingly allow JIT to be opened up to potential bad actors. Direct access to JIT features, or exploits involving JIT bugs, can make it easier for an attacker to write and execute unsigned unverified code. Accessing JIT has been involved in sophisticated attack chains that unleash new potential vectors for ransomware attacks, data theft, and other forms of malicious software to gain access to enterprise networks and put the security of the entire enterprise at risk.

If Apple were forced to open up this feature to any developer, it could lead to near catastrophic new security risks, give nation state threat actors a leg up, and put the integrity of core enterprise business operations at risk. Enabling weaknesses in an area where bugs are hardest to detect, where exploits are of the highest severity, in a place that is actively being exploited by nation state actors, and exploits that enable broad enterprise security risks for companies throughout Europe just doesn't make sense.

This JIT example follows in the footsteps of previous EC efforts to impose specific interoperability requirements on operating systems for competition purposes that ultimately led to a global IT outage,

crashing 8.5 million computers around the globe. This notorious outage led to the grounding of airline flights, knocked banks and media outlets offline, and disrupted hospitals, retailers and other services. Europeans need to buckle up, because unless DMA regulators change course, the worst is yet to come.

ANTI-STEERING AND LINK-OUTS

Another major digital disconnect in the EU's digital rules involve Article 5(4) of the DMA, which requires gatekeepers to allow apps to use external web links to "link-out" to communicate, promote, and use alternative payment mechanisms instead of trusted app payment systems provided by mobile platforms.

91% **OF CYBERATTACKS BEGIN WITH PHISHING**

80% **OF GLOBAL MOBILE PHISHING ATTACKS TARGET EU CITIZENS**

Link-outs to external websites are a well-known exploitable security vulnerability – especially when they link to unvetted, unverified websites that don't belong to the app developer itself. This is especially concerning given that there is a multibillion industry aimed at tricking people into clicking on things we shouldn't -- what experts call phishing. In fact, 91% of cyberattacks begin with phishing – and 80% of global mobile phishing attacks target EU citizens (54 million individuals), according to BICS.

Mandating unrestricted link-outs can enable threat actors to harness these links to distribute malicious sideloaded apps, hijack accounts via fake login pages, expose users to fraudulent scams, or deploy spyware undetected. Because of these types of cyber risks, Europe's Cyber Resilience Act (CRA) requires smartphones to "be designed, developed and produced to limit attack surfaces, including external interfaces." These protections were built into established app marketplaces. But under the DMA, platforms are being restricted from protecting users from scammy links. Even more concerning, the EC has mandated that Apple is also not allowed to protect against links with vulnerable redirects -- a known exploitable vulnerability – even though the CRA requires "Products with digital elements shall be delivered without any known exploitable vulnerabilities."

Another significant privacy and security risk the DMA has imposed is requiring mobile platforms to allow URLs to include passed parameters information. But doing so can expose sensitive information including PII, user identities, session tokens, API keys, or any other data stored on a phone. So while DMA regulators are fining Apple for its effort to protect that PII from being passed, DMA regulators are requiring Apple to allow external links that contain any amount of PII and other information to be transferred outside of the EU to any external website in any country, even to a website that doesn't even belong to the app developer. Regulators are requiring this despite the fact that Europe's flagship privacy law GDPR imposes restrictions on the transfer of personal data outside the European region.

Consumers are also likely to be unaware that using these outside links would impede their ability to seek redress in the event of a scam or fraud. That's because key app store features like Report a Problem, Family Sharing, and Ask to Buy — will not reflect these link-out transactions – making it harder for the platform to refund customers that may encounter scams or fraud.

Lastly, even though EC government websites, investment firms, banks, and others regularly use external link disclaimers to warn users when they are leaving and going to an external website, the DMA's regulators are prohibiting Apple from doing so. When Apple proposes to include its own external link disclaimer, the EC claims that the disclaimer "is not neutral and objective and thereby may deter end users from exercising their right under Article 5(4)", and has fined Apple.

BUT WHAT DO EUROPEAN CONSUMERS WANT?

OF CONSUMERS IN SOUTHERN EUROPE WOULD LIKE TO RESTORE PRE-DMA SERVICES

and they would even be willing to pay a premium to get them back

55% of higher-income consumers

52% of lower-income consumers

WOULD BE WILLING TO PAY MORE TO RESTORE PRE-DMA TECHNOLOGY
to ensure safe payments for gatekeeper operated app marketplaces

#1 it's the number one priority for higher earners

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.

The irony here is that Apple is seemingly being fined for using the same kind of warning messages to protect users that the EC itself uses, for requiring the same kind of consumer privacy and security safeguards as the EU's GDPR and CRA require, for using markups for items on its store shelves that are a fraction of what are commonly found on store shelves throughout the EU of 15% to 60% on average, and for providing a trusted app payment system that Europeans want. But no good deeds go unpunished. It's another example of the DMA's digital disconnect, how compliance exposes Europeans to increasingly ubiquitous, effective, and especially harmful threats including malware, phishing, and fraud -- driving Europe straight into the digital danger zone.

SIDELOADING'S SIDE EFFECTS

One of the prominent requirements of the DMA is to allow apps to be directly installed from the web or from alternative app marketplaces. Sideloading can allow users to access apps that are unavailable in their region for legal reasons, that do not meet official app marketplace standards of excellence, or that perform illegal activities such as bypassing copyright protections. While this sounds reasonable in theory, in practice, this requirement – sideloading – creates enormous risks for users.

The DMA's mandate to allow sideloading and break open the controls of official app marketplaces has opened the gates to a broad

range of user harms and exploits. Over 95% of malicious Android apps originate from sideloading, not from the official Play Store. Users who engage in sideloading are 80% more likely to have malware running on their devices compared to those who do not, according to Zimperium. Likewise, data security experts believe unverified app stores are key vectors for some of the biggest mobile threats including banking trojans, spyware, and counterfeit apps mimicking legitimate services to steal credentials.

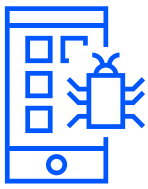
> THE DMA REQUIREMENTS REDUCE THE ABILITY TO RESPOND TO AND REMOVE MALICIOUS APPS, AND TO ANTICIPATE NEW AND EMERGING THREATS BEFORE THEY ARE ALLOWED ON THE PLATFORM.

The DMA's required changes also break the system of software patches and updates that are integrated into official app marketplace governance models, prevents the platform from taking down apps for content reasons (even if flagged by a trusted flagger set up under DSA provisions), or if the app's developer uses a common bait and switch tactic to morph the capabilities of the app into something else once installed for nefarious outcomes. Although platforms have adopted a notarization scheme to help address and reduce some privacy and security risks by reviewing sideloaded apps in advance, the DMA requirements reduce the ability to respond to and remove malicious apps, and to anticipate new and emerging threats before they are allowed on the platform.

These risks come at a time when mobile malware threats are surging across Europe. Researchers from Proofpoint detected a 500% jump in mobile malware in Europe alone, largely because of Android's approach to sideloading which, as they report, makes the "platform popular with bad actors, who know that Android phones can be compromised in just a few steps."

These significant changes are especially impactful for Europe's businesses. As the EC forces the requirement to allow sideloading on all mobile devices, it prevents enterprises from choosing the most secure option. This creates an insecure enterprise mobile environment where unvetted and sideloaded apps become threat multipliers and potential vectors for ransomware attacks, data theft, and enabling other forms of malicious software onto the network putting the security of the entire enterprise at risk. Google reports that apps downloaded from outside its app store are 50 times more likely to contain malware. By extending these threats across the entirety of Europe's mobile ecosystem, the costs could be staggering. As we describe in this report, a single mobile malware exploit could cost individual European businesses as much as $150 million to recover from.

A SINGLE MOBILE MALWARE EXPLOIT COULD COST INDIVIDUAL EUROPEAN BUSINESSES AS MUCH AS



$150 MILLION

TO RECOVER FROM

TRUSTED FUTURE

IMPEDING COMPETITION:

INTENDED TO BOOST COMPETITION, THE DMA IS NOW IMPEDING IT

October 2025
Failed Experiment
Report 1_4

IMPEDING COMPETITION: INTENDED TO BOOST COMPETITION, THE DMA IS NOW IMPEDING IT

One of the fundamental flaws in the DMA's framework is that rather than targeting demonstrable competition failures and their resulting consumer harms, the DMA instead targets companies based on artificial user and revenue thresholds.

By focusing merely on platform size to encourage competition, rather than specific consumer harms, the DMA has:

Ignored the important economic and consumer benefits that Europe obtains from the already dynamic and vibrant smartphone marketplace and the broader app ecosystem it enables.

Underappreciated how a resultant tech gap (led by an AI tech gap) is now leaving European consumers and innovators behind, less able to compete with global counterparts.

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 prevent their good ideas from being copied by others.

Disregarded how the expansive mandated security weaknesses it has driven into Europe's technology ecosystem place 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.

Disregarded the important and vital role that trust plays as a differentiator in enabling competition. Economic competition is enabled by privacy, safety, and security standards that people want and that policymakers have been trying to foster for decades. But the DMA degrades this critical form of competition.

ignored the often more important elements that enable vibrant, innovative, safe, and secure and dynamic competition on digital platforms.

> IN EFFECT, BY TRYING TO OPEN UP APP MARKETPLACES, THE DMA HAS INADVERTENTLY WALLED OFF EUROPE'S APP INNOVATION ECOSYSTEM.

We've already seen how a vibrant, dynamic and competitive app economy has led to an explosion in new business, new types of business models, and economic gains both online and offline throughout Europe. As previously described in a European Parliamentary Research Service (EPRS) report on the European app economy, app stores have lowered, not raised, the barriers to entry.

A primary DMA goal is to lower barriers and foster new competition. But 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, 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.

Likewise, Europe's growing AI app gap – which was also created by Europe's new digital rules – is leaving European app developers less able to compete internationally. Outside of Europe, developers are using AI tools and "vibe coding" techniques to speed up coding and debugging, develop game music, and create more compelling and immersive graphics for games. In other countries, a wider variety of AI tools is helping boost app competition by even allowing small developers with no previous coding or software skills to create apps that can compete in the global app economy. But European developers face hurdles due to regulations like the DMA. For example, interoperability rules have prevented Europeans from accessing Apple Intelligence, which also prevents Europeans from taking advantage of game-changing new features like real-time translation directly through earbuds. If European businesses can't access these translation features, it puts them at global disadvantage with other businesses who can more easily transact business around the world. In effect, by trying to open up app marketplaces, the DMA has inadvertently walled off Europe's app innovation ecosystem. Together with other EU rules, the DMA is also walling off Europe not only from the AI tools its app developers need to better compete, but that Europe needs to be more competitive.

It's not just European app developers hurt by these requirements. The security weaknesses that come with DMA enforcement have created significant costs for companies in almost every sector of the economy that must now increase spending to better defend their security and networks. It can cost organizations with 10,000 employees as much as $35 million per cybersecurity incident and up to $150 million per incident for organizations with 50,000 mobile devices. For small businesses, the average cost of a mobile cyber-attack can range between $120,000 and $150,000. These costs are more likely to accrue to Europe's rank and file businesses, and less likely to accrue to Europe's competitors. While DMA regulations may marginally benefit a handful of vocal (often non-European) app developers, it undermines the vast number of European businesses struggling to compete and win in today's global economy.

These regulatory changes neither advance fairness nor competition –the core tenets the DMA intends to advance. Europe's regulatory moves have delayed innovations, degraded services, and impeded developers from offering new kinds of AI enabled app innovations – creating second class digital citizens.

HINDERING POTENTIAL: A BETTER PATH TOWARDS EXPANDING EUROPE'S ECONOMIC POTENTIAL

Rather than fostering a vibrant and secure digital ecosystem, the DMA has seriously impeded Europe's digital economic potential. Instead of fostering competition and growth, in effect, the DMA has turned Europeans into second class digital citizens by delaying innovations, degrading services, and undermining key privacy, safety and security safeguards.

Europe's slow technology adoption rates combined with a tsunami of sometimes contradictory new technology regulations like the DMA have converged to create one of the biggest barriers to its future economic and consumer gains. In sounding the alarm on Europe's expanding technology gap, McKinsey found large European companies are now 20% less profitable than their American counterparts with 90% of the gap attributable to technology-creating industries. They warn that unless Europe closes its technology gap, European firms across broad sectors will likely be put at a competitive disadvantage, jeopardizing Europe's long-term prosperity.

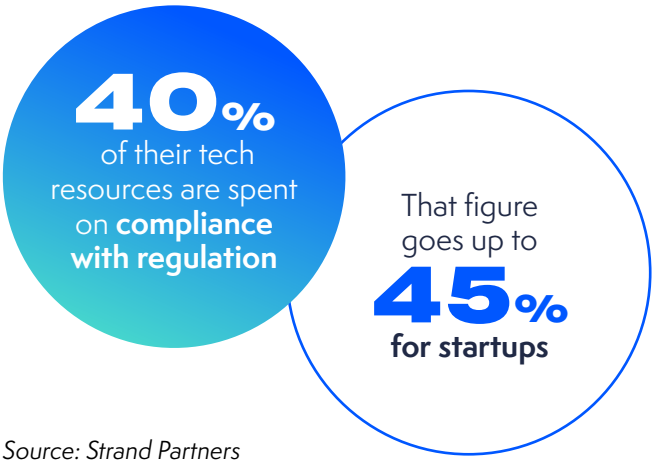
> DESPITE ITS GOOD INTENTIONS,THE DMA IS TRIGGERING MAJOR ECONOMIC LOSSES OF AS MUCH AS **€114 BILLION** FOR FIRMS ACROSS THE BROADER EU ECONOMY.

The good news is that if Europe can foster a more innovation-friendly environment, take a more informed and consistent approach to its regulatory frameworks, and close its growing technology gap it could help lift nearly every sector of the European economy. An analysis by Accenture finds Europe could generate a staggering €3.2 trillion in additional economic gains by adopting this approach.

A lack of trust in technology is one of the biggest barriers to closing this technology gap in Europe. Despite its good intentions, the DMA is triggering 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.

In fact, Europe's broad approach to regulation is shackling its unique potential. An analysis by Strand Partners found EU businesses estimate that 40% of their tech resources are spent on compliance with regulation. That figure goes up to 45% for startups.

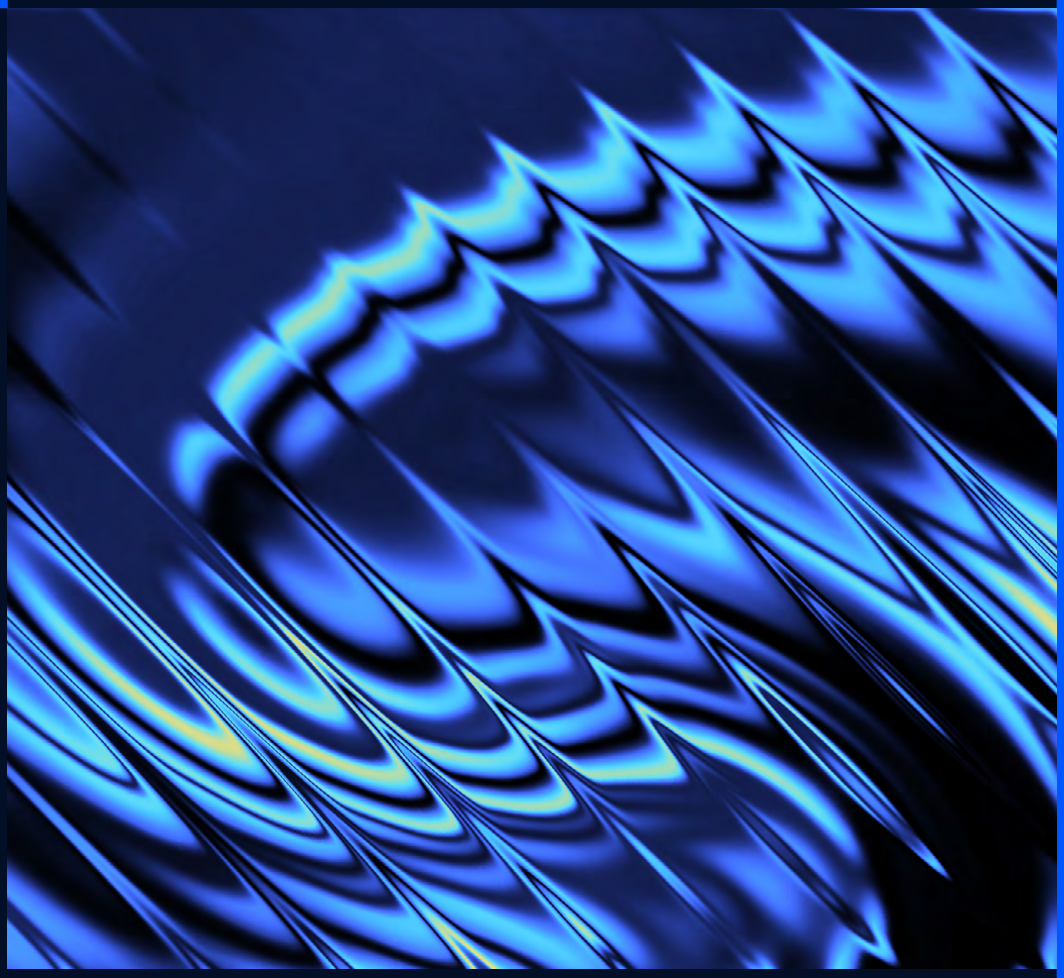
↗ EU BUSINESSES ESTIMATE THAT



Source: Strand Partners

The Center for Strategic and International Studies estimates that the DMA and DSA 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. This data points to crippling factors for Europe's tech industry, with regulations driving away the investment that the EU badly needs and choking the growth of its most promising scaleups.

TRUSTED FUTURE



RECOMMENDATIONS

October 2025
Failed Experiment
Report 1_4

RECOMMENDATIONS

TO MAKE THE EU'S DIGITAL POLICIES WORK, AND WORK TOGETHER WELL, THERE NEEDS TO BE A FUNDAMENTAL RE-THINKING AND RE-ALIGNMENT OF CORE DMA IMPLEMENTATION.

At SXSW, Former European Commissioner for Competition Margrethe Vestager, said her next policy priorities are straightforward: "Implementation, implementation, implementation... We need to show the world that we are not only good at negotiating and passing legislation, we are also good at making it work." That's laudable, but that is not what is happening now.

To make the EU's digital policies work, and work together well, there needs to be a fundamental re-thinking and re-alignment of core DMA implementation. More attention needs to be paid to implementing and aligning these frameworks in a user-centric way so they are consistent, effective, and synergistic in addressing the very real challenges the DSA, the DMA, the CRA, the GDPR, and Europe's security agencies were designed to address.

Europe stands at a critical digital crossroads: How Europe chooses to respond in this moment could be one of the most consequential decisions that shapes its long-term future. To move from technological laggard to leader, to crank up its economic engine, close its technology gap, and boost its long-term economic competitiveness, and unlock the previously unthinkable mobile opportunities that improve people's lives, Europe must fully embrace a more trusted technological future.

Policymakers in the EU, and around the globe, should take immediate steps to advance the following:

1

Countries looking to replicate DMA like policies should immediately pause efforts until they have a complete understanding of the DMA's full impact.

Europe has been running an experiment that is playing out right before our eyes. The question is not whether these regulations work – the data proves they do not. The real question is whether countries will learn from Europe's failed experiment or repeat their mistakes.

For those looking at replicating DMA-like proposals, like those being considered in Australia, Brazil, Canada, India, Japan, Turkey, South Korea, the U.K., and elsewhere, this report should be a red flag warning. They should pause their efforts until they can ensure that by opening up the existing trusted app-ecosystem, they aren't actually opening up a new Pandora's box full of broadly foreseeable problems. Having a complete and thorough understanding of these impacts is vitally important. Rather than exploring whether the EU's DMA mandates are actually leading to positive outcomes, and the steps they would need to take to overcome the significant shortcomings that are just now becoming understood – the EU has been encouraging other countries to follow suit and replicate the mandates merely because they have been imposed elsewhere. As a result, they are leading other countries down a risky path without ever having examined the vast shortcomings, conflicts, safety, security, privacy and other significant new setbacks that the new governance framework has also created.

2

The EU needs to launch a comprehensive public service campaign that warns mobile users and its technology enabled business of coming threats.

Given the tsunami of predictable expanded threats coming to Europe's mobile landscape and to the digitally enabled companies that depend upon mobile security, the EC has done too little to warn businesses, consumers, and government leaders about the advancing threats. It's not too late to launch a comprehensive public service campaign aimed at warning consumers about the growing risks of scams and frauds, to warn parents about new limitations to parental controls, to warn businesses about growing malware threats, and as cybersecurity experts have warned across the globe, warn mobile users to only download apps from official app stores.

3

The EU should make its regulatory reset count by recalibrating its digital framework to better align goals, drive a more trustworthy ecosystem, and strengthen the EU digital economy.

As the landmark Draghi report rightly identifies, an abundance of conflicting mandates and overregulation have become barriers to European competitiveness. A forthcoming regulatory simplification package presents an opportunity for the EU to recalibrate its digital regulatory framework to support competitiveness, innovation and international coherence.

4

Europe must swiftly address the DMA's inherent digital disconnects in order to advance Europe's efforts aimed at advancing a more vibrant, competitive, and trustworthy digital ecosystem.

Europe also needs to retarget its digital markets mandates to address actual consumer harms, with evidence-based solutions that specifically address these harms to produce corresponding consumer benefits. DMA regulators say they will keep up with changing dynamics by carrying out market investigations and then they will: "update dynamically the obligations for gatekeepers when necessary." However this report and analysis makes clear that the need to update its rules are already urgent and necessary. The DMA's rules go far beyond what the law requires, lack alignment, and are setting back Europe's ability to solve some of Europe's most important technological challenges – issues around advancing a more trusted digital future that the DSA, CRA, and GDPR (among others) are attempting to advance. The Commission should embark on an effort to implement, enforce and align these frameworks in a user-centric way so they are consistent, effective, and synergistic in addressing the very real challenges the DSA, the DMA, the CRA, the GDPR, and Europe's security agencies were designed to address.

5

Regulators must take full advantage of DMA provisions that can advance a more trusted digital future.

To achieve the DSA's goal of advancing a more trustworthy digital ecosystem, DMA enforcers should not ignore the escalating privacy, safety and security threats in the mobile environment, resist efforts to dismiss gatekeepers' privacy and security enhancing governance measures as taken only to protect their self-interest and take responsibility for the alignment of their own rules with other rules. Article 8 of the DMA recognizes the potential for the many policy disconnects outlined in this paper. But it places the burden on platforms to make sure they are taking actions that are consistent with the GDPR and cybersecurity regulations. In doing so, regulators seem to believe they have absolved themselves of having to ensure that their own DMA rules are consistent with other

EU obligations and policy goals. But rather than taking a "hands off" approach, enforcers and platform providers should be encouraged to take full advantage of provisions in Article 6(4) of the DMA enabling gatekeepers to comprehensively protect the integrity of the hardware, and operating system, and to take measures "enabling end users to effectively protect security in relation to third-party software applications or software application stores." In addition, enforcers should fully leverage the discretion provided under Article 10 of the DMA to pause implementation of the multitude of problematic provisions outlined in this paper unless and until they can be sure the implementation will not expand harms and create new threats. Platforms should not be fined or punished for implementing the DMA in a way that both meets the requirements in the law and balances the need to protect security, critical networks, election integrity, children's privacy, limits fraud, abuse, and inappropriate content. If obligations are applied too strictly or inconsistently, a host of pro-competitive conduct will be prohibited. There is, however, ample room in the DMA's enforcement regime under Article 8(3) to take account of "the specific circumstances of the gatekeeper.

6

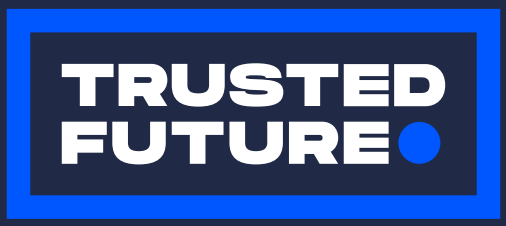
Regulators should invest in their own technical and cybersecurity expertise to improve implementation.

EC leaders need to swiftly make major new investments in hiring the substantial increases in expert technical, legal, policy and oversight personnel necessary to effectively and consistently review and implement its laws in a more cohesive and effective way. The EU reportedly has just 80 people working to implement the DMA and often lacks both the breadth and depth of technical, cybersecurity, economic and other expertise necessary to evaluate its far-reaching rules and their implementation. By one measure, the city of Brussels has double the number of staff devoted to parking enforcement alone. It's also become especially clear that it lacks baseline security expertise on hand that can engage Europe's national security and cybersecurity expertise. Having this breadth and depth of technical expertise on hand is essential for policymakers to be able to engage in a meaningful regulatory dialogue that can swiftly identify and resolve the many important issues where they need to square the circle.

7

Regulators need to commit themselves to following fair and due process.

Enforcers should ensure they use reasonable requirements that don't stray beyond the facts or the law, that are focused on curing actual harm with evidence-based solutions that work, that ensure consistency across statutory goals, and ensure any resultant fines are reasonable and proportionate. If these cases are to withstand likely legal appeals, regulators will need to take the time necessary to comprehensively review


TRUSTED
FUTURE