

# Security and Trust from an App Maker's Point of View

November 2021

## Executive Summary

- Small and medium-sized app developers and startups rely on consumer trust to compete with global brands on a level playing field. Building up consumer trust takes a long time and can make or break an app development company.
- Because consumers trust software distribution platforms, smaller, unknown app makers can gain almost instant consumer trust and access to a global market by having their apps available on these platforms.
- Legislative proposals like the Digital Markets Act may unintentionally put consumer trust at risk. Focusing on access and contestability in the DMA could make it hard for a platform to combat illegal content or uphold security and privacy standards, opening the gate for malicious actors.
- Sideloaded apps would allow apps to be available for download without a thorough investigation into their inner workings, making it easier for bad actors to pirate apps or install malware on consumers' devices accessing sensitive data and sensors on the device. As a result, consumers may stop trusting apps from unknown brands, which would be devastating for smaller app developers.
- The rigorous app review and security measures that the main software distribution platforms employ enable small developers to compete on the same footing as bigger companies with global name recognition.
- Preserving the current security environment on software distribution platforms is crucial to the success of SMEs and startups.

In just 14 short years, the app economy emerged out of nowhere to become an €830 billion ecosystem. Throughout the COVID-19 pandemic, the app economy thrived and played a key role in sustaining our work, studies, and daily lives. In particular, small app development companies, like ACT | The App Association members, drive the app economy and advance innovation every day.

Startups and smaller app makers are the most innovative engines of growth that improve our lives and make our business operations more efficient. However, merely creating innovative and useful apps is not enough – people must want to use these apps before they download them, even if they are not familiar with the company or brand behind them. For that, consumers need to trust the companies that make these apps, no matter their size. As the growth of the app economy demonstrates, app stores offer app makers a unique platform that empowers them with instant consumer trust and a global reach<sup>1</sup>.

For example, French App Association member company L'Escapadou consists only of founder Pierre Abel's family of four. Yet the app firm was able to secure more than 2.2 million downloads and earned over \$715,000 (approximately €619,000) in revenues from app store sales between 2019 and 2020<sup>2</sup>. Pierre says the centralised nature of platforms allowed him to be successful by helping him to reach a global audience. Without the app stores, it would be impossible for him to make a living selling exclusively to the French or European markets<sup>3</sup>.

In general, app developers build upon the range of services app store platforms and device makers offer and they benefit from the value these services generate, which include:

- Customer trust in apps from new and unknown brands;
- Immediate distribution to hundreds of millions of customers across the globe;
- Promotion and marketing channels through the platform;
- Platform-level privacy controls;
- Assistance with intellectual property (IP) protection;

<sup>1</sup> Read more about the beneficial relationship between app developers and software distribution platforms in the 2020 Deloitte study *'The App Economy in the European Union'*.

<sup>2</sup> Retrieved from Sensortower

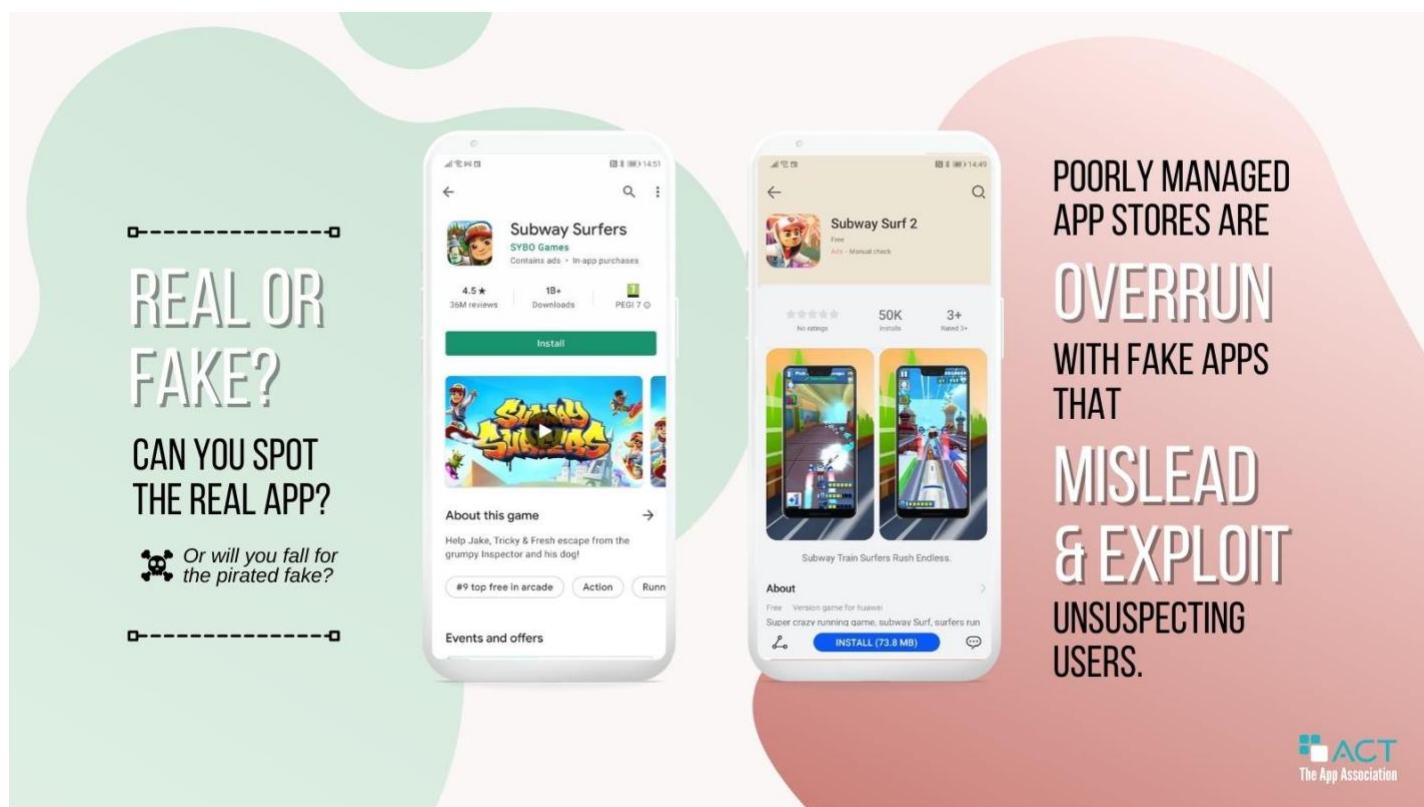
<sup>3</sup> For more information, see the App Association's *Member Spotlight* on L'Escapadou.

- Security protection and threat mitigation through operating systems and gatekeeping;
- Developer tools and frameworks, including accessibility features;
- Access to hundreds of thousands of application programming interfaces (APIs);
- Customer service, including payment processing, refund, and subscription management.

Consumer trust, security, and privacy are among the most essential features for smaller app developers. Consumers are more likely to trust global brands with name recognition like Pinterest, Spotify, or Uber than smaller companies and startups. Therefore, the latter rely on software distribution platforms to provide a trusted marketplace to their users. By both reviewing proposed apps and updating security for the device's operating system, software platforms ensure high levels of security and trust. The App Association has concerns that legislative proposals like the European Union's Digital Markets Act contain provisions that put these high levels of security at risk.

*'At WodPod, we're a team of three, and none of us are lawyers, so legal requirements are hard to navigate for us. By putting it on app stores, where users know it's safe, we easily reach consumers and instantly gain their trust'.*

– Mattia Carluccio (WodPod, Spain)



Visualisation by the App Association. Data <sup>4 5 6 7</sup>

<sup>4</sup> Munich Security Conference Security Proofing the European & Transatlantic Tech Agendas [discussion paper](#)

<sup>5</sup> The risks of third-party app stores, [Norton](#)

<sup>6</sup> Fake Mobile Apps: A Growing Threat, [Guardsquare](#)

<sup>7</sup> Cybersecurity company McAfee, for example, explicitly [recommends](#) avoiding third-party app stores to keep mobile devices secure.

## Consumers now place greater importance on privacy and security

Mobile phones, tablets, and wearables are the most 'personal' computers consumers own. These devices have cameras, access our physical location, store our medical and financial information, and are a medium for private and professional conversations. In short, mobile devices are a potential goldmine of personal data for malicious actors<sup>8</sup>. And yet, few of us have virus scanners on our mobile phones or dive into the source code before installing an app.<sup>9</sup>

Through careful gatekeeping and curation, platforms created an environment where people trust apps and routinely install them on their phones without hesitation. This trust took years to build. The same was true for software developers before the introduction of the smartphone and app stores: they had to break the trust barrier by handing their products to companies with more brand recognition. For example, in 2002, long before software distribution platforms, the French developers of the video game Heart of Darkness contracted with Kellogg's cereal to augment their consumer base in Germany.<sup>10</sup> Developers converted their game software to create a child-friendly demo that the cereal company usually affixed to its boxes. Today, consumers can download games like these for free on software distribution platforms, and they can also reach consumers beyond those who buy a particular brand of cereal or another trusted product.

In addition to competition between the platforms, app makers of all sizes compete directly on privacy. App Association member company Telemetry Deck, for example, runs a successful privacy-focused app analytics tool that allows developers to learn about app usage patterns, flows, and configuration, without putting their users' privacy at risk. Developers constantly work to meet and exceed consumer expectations while fulfilling compliance requirements of various privacy rules and structures. These privacy safeguards further foster a trusted ecosystem. Consumers are willing to trust apps they download from app stores because of years of positive experiences with the extra scrutiny and safeguards app stores offer. Simply being available on the app stores is now an indicator that an app is reasonably trustworthy for consumers. At the same time, app developers strongly desire platform-level privacy controls they can adapt for their products and services.

## The myth of choice for sideloading or multiple app stores

Much like most of us don't read the terms of service we routinely agree to, we also don't spend time researching the apps we download. In the current environment, that's okay because the platforms' developer guidelines include thorough reviews of each app submitted and other gatekeeping measures that keep our data safe and secure<sup>11</sup>. In addition, app stores offer parental controls and additional protections to prevent children from making unintentional purchases or restrict the sharing of personal information. These safeguards generated a system where consumers can confidently download an app of a company they don't know. Operators of popular software distribution platforms have worked years to earn this reputation and, therefore, have a strong incentive to maintain their trustworthiness and keep their platform from being compromised. Not only do alternative app stores lack the same incentives, but they also do not have the resources to do this. What would happen if no one checks apps anymore before they become available for download? If no one investigates the inner workings of an app before releasing it, bad actors will reign free, causing consumers to stop trusting apps from unknown brands.

*'While the idea of regulating platforms is the right one, our concern is that this legislation will change an ecosystem that works well into something that doesn't. [...] We need to be careful not to hurt small businesses that are entering the market by using platforms'.*

– Francesco Ronchi (Synesthesia, Italy)

<sup>8</sup> In 2020, [Kaspersky](#) detected 5,682,694 malicious installation packages, 156,710 new mobile banking Trojans, and 20,708 new mobile ransomware Trojans. Varonis published more mobile ransomware statistics [here](#).

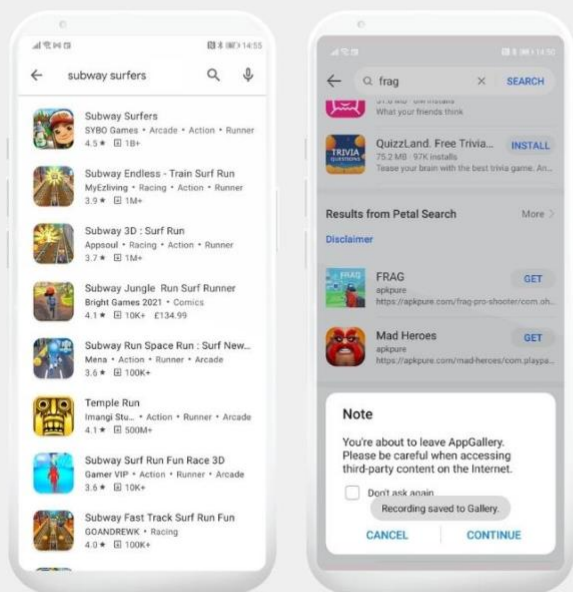
<sup>9</sup> In 2018, [Statista](#) estimated that only 1.3 billion mobile devices had installed antivirus software, a low number when compared to the 8.8 billion devices online in 2018 ([Cisco](#)). [Check Point](#) found that 97% of organisations faced mobile threats via various attack vectors in 2020, with 46% of organisations having at least one employee download a malicious malware application.

<sup>10</sup> Read more here (in German) on [pcgames.de](#)

<sup>11</sup> Cybersecurity company McAfee, for example, explicitly [recommends](#) avoiding third-party app stores to keep mobile devices secure.

If regulation forces platforms to allow sideloading and downloads from alternative app stores, as the Digital Markets Act intends to do, large and dominant players will likely make their apps exclusively available via sideloading or their own potentially less privacy-focused app stores. Such an environment would only benefit big name brand apps at the cost of small and medium-sized enterprises (SMEs) and startups. Additionally, reports show that third-party app stores have fewer safeguards than well-known app stores. On some of these alternative app stores, malicious apps even outnumber their safe offerings<sup>12</sup>. Lowering current privacy and security protections will increase the likelihood of invasive tracking, fraud, malware, theft, and piracy. For example, what looks like the same app on another distribution platform could actually be a different app, with the sideloaded version being a trojan horse that tracks users, steals information, or malfunctions<sup>13</sup>. This situation is bad for consumers and further erodes the trust in apps on which smaller app makers depend.

## FAKE OR REAL? IT'S HARD TO TELL THE DIFFERENCE









Fake and pirated apps are listed **alongside** the real app in some third-party app stores.


Even if you think you've found the real thing, some app stores **redirect to fake apps** if real ones are not on there.

**Third-party app stores have too few checks. Sideloaded has no checks at all.**

## HOW THIS AFFECTS DEVELOPERS

-  **Losing revenue**
-  **Harming our brands severely**
-  **Endangering users that think they have the real version**
-  **Compromising the security of our apps & servers**
-  **Losing valuable time**
-  **Requiring expensive additional server capacity**

Featured REAL apps are made by our members.



Visualisation by the App Association. Data<sup>14 15 16 17</sup>

## How piracy and ransomware harm both users and businesses

Pirated apps and ransomware are not only harmful to consumers, but a seemingly trustworthy app that turns out to be a pirated version or a trojan horse that downloads spyware and malware onto a consumers' phone can also destroy a developer's reputation. Malicious actors steal legitimate applications, remove their copyright protections, and place the apps in illicit stores for download, and no revenue goes to the original developer. What makes this situation even worse is that pirated apps may even continue to use the developer's servers and support services, adding additional and ongoing costs to the loss of revenue. Users may not be aware their personal information is at risk, or that their device is being used for other purposes, such as mining cryptocurrency, activating camera and microphone, and tracking keyboard strokes. From 2013 to

<sup>12</sup> In 2020, *RiskIQ* monitored both the well-known stores like the Apple App Store and Google Play and more than 120 secondary stores around the world.

<sup>13</sup> See, for example, the 2021 *Android Trojan*, a malware campaign that spread through social media hijacking, third-party app stores and sideloaded applications and hit 10,000 victims.

<sup>14</sup> Munich Security Conference Security Proofing the European & Transatlantic Tech Agendas *discussion paper*

<sup>15</sup> The risks of third-party app stores, *Norton*

<sup>16</sup> Fake Mobile Apps: A Growing Threat, *Guardsquare*

<sup>17</sup> Cybersecurity company McAfee, for example, explicitly *recommends* avoiding third-party app stores to keep mobile devices secure.

2018, mobile publishers lost \$17.5 billion (approximately €15 billion) in revenue due to app piracy<sup>18</sup>. One prominent example is the case of App Association member company Kiloo, developer of the popular game Subway Surfers, which lost \$91 million (approximately €78 million) in revenues due to pirated versions<sup>19</sup>. Sideloaded apps likely have not gone through any security reviews and alternative app stores may not implement review processes comparable to those of the main software distribution platforms. Therefore, the risk of downloading a pirated and potentially malicious app increases significantly if users sideload it or download it from an alternative app store.

Developers and small businesses look to the platforms to help protect their intellectual property and maintain the standards of quality and security that customers have come to expect from the software they download from app stores. Well-known platforms provide dispute resolution mechanisms for developers when outright copies of their apps, or apps that do not have the proper use license, appear on the app stores. Without these mechanisms, developers may face expensive copyright infringement litigation in international courts, leaving the legitimate IP owner with thousands of euros in legal fees, and diverting months or years from company matters. If sideloading or alternate app stores exist without safeguards and legal resources, small developers no longer have a means to effectively fight this existential threat.

*'Something we worry about is the ability of users to install apps from outside an app store environment. I remember the time before app stores. We had a lot of issues with piracy. We were basically competing with our own product that was offered illegally. As a business, it's really hard to compete with that'.*

– Karim Morsy (algoriddim, Germany)

## Conclusion

Small app developers depend on consumer trust. Without it, consumers will not download their apps, sticking to apps from known and established brands. Gatekeepers maintain security and privacy to help developers of all sizes gain this trust and thrive in the app economy. Rigorous app review and security measures enable small developers to operate and compete on the same footing as bigger brands with global name recognition. It is crucial to the success of SMEs and startups that we keep out bad actors by preserving the current security environment on software distribution platforms. The current security environment is not broken and forcing software distribution to allow sideloading and downloads from alternative app stores would only cause harm. Too rigid a regulatory approach, such as the one currently proposed in the Digital Markets Act, may unintentionally harm those actors who need the most support and rely on certain aspects of the current app ecosystem to succeed. In fact, the Munich Security Conference recently published a discussion paper that addresses the negative unintended consequences that are possible when policymakers do not consider the privacy and security implications of proposed regulations<sup>20</sup>. Neither consumers nor small app developers should operate in a less secure environment than we currently have.

## Recommendations for legislators:

- Focus on improving access conditions to existing platforms rather than mandating software distribution platforms to open up their whole systems at the cost of security. Instead, a careful, case-by-case analysis based on competition law should precede such actions.
- Ensure that access rules take into consideration the security, safety, and privacy of all users, and allow gatekeepers to continue upholding user trust and enable them to keep innovating to do so.
- Implement a more flexible obligation than the current Article 6 (c) DMA. The DMA is an important step in making gatekeepers accountable for their business practices and sets out the first framework to formally govern relations in the rapidly evolving platform ecosystem. To avoid unintended consequences that would harm SMEs, the principle of

<sup>18</sup> In a 2018 Forbes magazine article, "The Mobile Economy has a \$17.5B Leak: App Piracy," the author quoted an estimate from Tapcore that mobile publishers had lost \$17.5 billion in revenue over the previous five years.

<sup>19</sup> See Business Wire's [Smart Phone/Tablet Games Global Market Report 2021](#) for more information.

<sup>20</sup> Munich Security Conference [Security Proofing the European & Transatlantic Tech Agendas](#) [discussion paper](#)



secure access to various technologies should form the basis for these obligations, rather than focusing on unrestricted access to applications and application stores.

- Consider the valid reasons why a platform model that is more protective of the user experience may be preferable to a system without gatekeeping, especially in terms of user security, consumer protection, privacy, and data security.