Loyola Consumer Law Review

Volume 34
Issue 3 *Symposium Issue 2022*

Article 9

2022

Misplaced Trust, Failure of Contract, and the Need to Create Robust Options for Consumers

Anjanette H. Raymond
Kelley School of Business, Ostrum Workshop

Inna Kouper
Luddy School of Informatics, Ostrum Workshop

MISPLACED TRUST, FAILURE OF CONTRACT, AND THE NEED TO CREATE ROBUST OPTIONS FOR CONSUMERS

Anjanette H. Raymond[*] *and Inna Kouper*[**]

ABSTRACT

Platform and application 'marketplaces' (app stores) serve an important function for the consumer. The 'marketplace' serves a single point of choice for applications that will be downloaded, and used, on either the apple or android cell phone. Over time, consumers have been reliant- almost dependent on these marketplaces. One can easily imagine, consumers trust the host, they trust the marketplace, they trust the ongoing updates and other technology 'fixes' when their applications begin to fail- one is undoubtedly aware of the loyalty that exists to these brands and marketplace hosts. Exercising full control, app stores engender extreme loyalty and high trust.

The application marketplace is interesting in many dimensions when examined as a closed universe environment. For example, such a marketplace has barriers to entry for developers, and strong rules for participation, including technical specifications and specific limitations to price, and use of data. In addition, the users have barriers to entry as well. They must have accounts and would likely only enter if they have a compatible device. Despite this incredibly closed, highly regulated, marketplace the main authority/host/owner of the marketplace has demonstrated time and time again that they do not monitor marketplace developers, nor do they generally remove big player developers for violating the terms of entry.

---

[*] Weimer Faculty Fellow, Kelley School of Business; Director, Program on Data Management and Information Governance, Ostrom Workshop. All opinions are those of the author.

[**] Luddy School of Informatics, Computing and Engineering, IU Center for Survey Research, Ostrom Workshop

Situations such as this are a violation of consumer trust, trust that is misplaced, because the reliance upon information should be viewed as unreasonable based on the limited and misleading information that is available. Thus, this area is ripe for regulation as consumers are being misled and, in the process, are subject to manipulation.

In this paper we explain the more impactful issues that arise when a consumer decides to enter- and remains captured- in an application marketplace. The paper explores online marketplaces, both in general and specific. The paper then briefly explores the marketplace from the view of regulatory failures and asserts that these failures are essential business choices in design and behavior that leads to consumer lack of understanding. Suggesting that the marketplace gatekeepers should be held to these promises. The authors build the case for both trust and trustworthiness as essential in these marketplaces. Thus, the absence of monitoring and enforcement of rules does nothing but further erode consumer trust. The paper concludes by suggesting regulatory additions that are first steps in rebuilding a consumer's trust in digital application marketplaces.

I. ONLINE MARKETPLACES

A. Online Marketplaces in general

Online marketplaces are e-commerce websites that enable third parties to sell or distribute their products and services. The sellers and consumers can use several unified services provided by the marketplace, including account and payment management, broader advertising, and a greater selection of goods and customers. The marketplace operator charges a fee, which can be placed on the sellers or distributed among sellers and buyers. Since 2014 the online marketplaces have exploded and created many new categories of e-commerce, from short-term rentals to food delivery to freelance work exchange.[1]

---

[1] See Glenn Laumeister, Why Online Marketplaces Are Booming, Forbes, (April 20, 2014) available at https://www.forbes.com/sites/groupthink/2014/08/20/why-online-marketplaces-are-booming/2/

The success of online marketplaces has also stirred legal challenges and controversy. For example, in 2012 the Federal Trade Commission (FTC) undertook an investigation into Google's anticompetitive conduct for its use of exclusionary search and search advertising agreements and forcing companies to stop developing competing products and services.[2] Despite the agency failing to bring a case at the time, the controversy stimulated further action. For example, the *American Innovation and Choice Online Act*[3] would prevent big tech firms from giving preference to their own products and services. Like Amazon ranking its Amazon Basics product line above those of its competitors or Google serving up its own map results over Apple's. According to some lawmakers, moves like these unfairly stifle competition- and these efforts are often centered in those arguments surrounding antitrust and evaluate the business as an entire entity.[4]

While many antitrust conversations are applicable to both the online and app marketplaces, this article takes a narrower view and looks at the application marketplace as an arena ripe for regulation.

B. Application Specific Marketplaces

Application (or 'app') marketplaces or stores are similar to more general online marketplaces, but they restrict their services to distributing software and applications. Used predominantly in a mobile context, they are also used on the web, in gaming and in desktop environments (e.g., Microsoft app store). App marketplaces allow third-party developers to provide a unified experience to the users, including download and installation, payments, encryption, and other services. App stores are controlled and curated by their owners (hosts) and require the apps to go through a review and approval process. A wide variety of digital products can be sold through application marketplaces. These include

---

[2] See Johannes Munter, FTC's Google Memos Underline the Need for Legislation to Balance the Online Marketplace. News Media Alliance, (March 30 2021), available at https://www.newsmediaalliance.org/ftcs-google-memos-underline-the-need-for-legislation-to-balance-the-online-marketplace/

[3] S.2992 - American Innovation and Choice Online Act, 117th Congress (2021-2022) available at https://www.congress.gov/bill/117th-congress/senate-bill/2992/text?r=60&s=1

[4] Antitrust laws are regulations that encourage competition by limiting the market power of any particular firm.

business-to-business (B2B) software, such as Microsoft 365 and Google Workspace and of course, consumer apps such as games for iOS and Android devices.

The marketplaces are, in general, very large and contain a diverse number of offerings. For example, Apple's iOS controls 25% of the global smartphone market. While the other 75%, is largely controlled by Google's Android. Just considering the Apple marketplace, over a billion people are customers within the marketplace and in these situations, the only way to install apps is through the App Store. In fact, in the US Apple's market share approaches 50%. It is thus, not surprising that Apple has enormous influence over the way software is created and consumed around the world.[5]

According to Apple, the App Store is the place that consumers can trust to find safe apps that uphold the highest standards for privacy and security:

> For over a decade, the App Store has proved to be a safe and trusted place to discover and download apps. But the App Store is more than just a storefront — it's an innovative destination focused on bringing you amazing experiences. And a big part of those experiences is ensuring that the apps we offer are held to the highest standards for privacy, security, and content. Because we offer nearly two million apps — and we want you to feel good about using every single one of them.[6]

Do understand, there is no longer much of an argument that these are not classified legally as marketplaces. One of the expressions of power of app marketplaces is their fee structure. Thus, Apple charges $99/year to join their iOS Developer Program to be able to publish one's app for the iPhone, iPod, and iPad. If the app is a for-fee app, Apple charges 30% of the revenue.[7] Google changes a one-time fee of $25

---

[5] Andy Yen, How Apple uses anti-competitive practices to extort developers and support authoritarian regimes, Proton Mail, (June 22, 2020) available at https://protonmail.com/blog/apple-app-store-antitrust/

[6] Apple Store Website available at https://www.apple.com/app-store/ (last visited April 17, 2022)

[7] See Apple Store, Developer Enrollment webpage, available at https://developer.apple.com/support/enrollment; Apple Store, Developer Explanation webpage, available at https://developer.apple.com/programs/whats-included/ (last visited April 17, 2022)

and then 15-30% or revenue as well.[8] This high revenue percentage has now become the subject of antitrust investigations in both the United States and the European Union when Spotify accused Apple of using their dominant position to influence the music streaming services market.[9]

II. FAILURES IN THE ONLINE MARKETPLACES

When a user installs an app from the app store, permissions are requested prior to installation, and, depending on the versions of the phone and the OS, the choice can be all-or-nothing or selective. Over the years, both Apple and Google added a more developed system of permissions than before, allowing users to grant permissions selectively and either once, while the app is in use, or all the time.[10] Knowing how permissions work, however, requires some technical knowledge from the user and a higher degree of involvement. Moreover, it is not clear whether every data type is included in explicit management of permissions.

Each mobile device contains a wealth of sensitive information that third-party apps can request, including the unique phone identifier (IMEI), contacts list, location, text messages, contents of personal files, proximity, temperature, acceleration, and other sensors, and so on. In 2013 one study found that a total of 101 different types of permissions were requested from android phone users, including full network access, ability to modify or delete content, and access to phone status and identity.[11] While some of these were necessary to the app's work, most of them were not and invaded user's privacy.

---

[8] See Google Play, developer answers, website available at https://support.google.com/googleplay/android-developer/answer/10632485?hl=en&ref_topic=3452890 (last visited April 17, 2022)

[9] See Tom Warren, EU accuses Apple of App Store antitrust violations after Spotify complaint, The Verge, (April 30, 2021), Available at https://protonmail.com/blog/apple-app-store-antitrust/ (last visited April 17, 2022)

[10] See Ben Stegner, What Are iPhone and iPad Permissions, and How Do They Work?, Make Use Of (MUO) Nov 5, 2021, https://www.makeuseof.com/iphone-ipad-permissions-how-do-they-work/; Android Developers Website, Permissions on Android https://developer.android.com/guide/topics/permissions/overview (last visited April 17, 2022)

[11] See N. S. A. A. Bakar and I. Mahmud, "Empirical Analysis of Android Apps Permissions," *2013 International Conference on Advanced Computer Science Applications and Technologies*, 2013, pp. 406-411, doi: 10.1109/ACSAT.2013.86.

In fact, many apps (over 60% of paid and 90% of free apps) are connected to trackers that collect personal information with apps often being connected to more than one tracker and many users being exposed to more than 25 trackers, which results in significant leakages of privacy.[12]

These apps, in their various environments, are not merely privacy destroying. They are part of an ecosystem that demands loyalty to the platform, misleads or otherwise intentionally subverts the acquisition of knowledge needed to make a reasonable choice about the way the environment behaves, and information is collected, and selectively enforces terms- those users of the app ecosystem assume are part of the protections within the environment.

A. Specifically Beholden to App Stores

As readers are undoubtedly aware, for a significant period of time the Google Play Store has easily allowed users of the Android phone to sideload apps.[13] Yet, Apple prevents the sideloading of iPhone apps, claiming the practice would make its phones less secure and trustworthy for users.[14] Many argue, the choice of Apple to prevent the sideloading of apps is but one example of a robust mechanism of creating a marketplace that significantly restricts, monitors, and enforces terms, to its own benefit.[15] The point is a hallmark of the EU's proposed Digital Markets Act (DMA) which is seeking to potentially compel

---

[12] See Suranga Seneviratne, Harini Kolamunna, Aruna Seneviratne, A measurement study of tracking in paid mobile applications, Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks, June 2015 Article No.: 7, Pages 1–6https://doi.org/10.1145/2766498.2766523 available at https://dl.acm.org/doi/10.1145/2766498.2766523

[13] For the most part, sideloading is downloading an app from outside the traditional marketplace. See Joe Fedewa, How to Sideload Apps on Android, How To Geek, (Jan, 28, 2022) available at https://www.howtogeek.com/313433/how-to-sideload-apps-on-android/ (last visited April 17, 2022)

[14] Apple Authors, Building a Trusted Ecosystem for Millions of Apps, (June 2021) available at: https://www.apple.com/privacy/docs/Building_a_Trusted_Ecosystem_for_Millions_of_Apps.pdf (last visited April 17, 2022)

[15] Joe Porter, Apple argues against sideloading iPhone apps as regulatory pressure mounts, The Verge, (June 20, 2021) available at https://www.theverge.com/2021/6/23/22546771/apple-side-loading-security-risk-report-regulatory-pressure (last visited April 17, 2022)

Apple to allow sideloading of apps[16] and something that Congress has taken on itself, in several ways in hearings.[17]

The heart of this debate can be seen in the Epic games case, in which Apple removed the Fortnite app from its marketplace.[18] Apple took this action when Epic games included a new feature, one that allowed consumers to pay Epic games directly for in-app currency, rather than paying in the traditional way, via the Apple payment mechanism.[19] In its lawsuit filing, Epic claims that Apple had become a "behemoth seeking to control markets, block competition, and stifle innovation."[20] And "far exceeds that of any technology monopolist in history."[21] Of course, Google shortly after also pulled the Fortnite app from its marketplace[22] and has now been sued as well.[23]

Of course, it is not merely that the marketplace is monitored and controlled by Apple, or Google or Sony; it is also important to recognize the cost of entering the marketplace and the cost of moving into a new

---

[16] Joe Porter, Apple argues against sideloading iPhone apps as regulatory pressure mounts, The Verge, (June 23, 2021) available at https://www.theverge.com/2021/6/23/22546771/apple-side-loading-security-risk-report-regulatory-pressure (last visited April 17, 2022)

[17] Makena Kelly, House lawmakers introduce five bipartisan bills to unwind tech monopolies ,The Verge, (June 11, 2021) https://www.theverge.com/2021/6/11/22529857/democrats-antitrust-big-tech-facebook-amazon-google-apple-competition-package-bills (last visited April 17, 2022)

[18] Malcolm Owen, Epic Games vs Apple trial, verdict, and aftermath - all you need to know, Apple Insider (AI), (March 26, 2022) available at https://appleinsider.com/articles/20/08/23/apple-versus-epic-games-fortnite-app-store-saga----the-story-so-far (last visited April 17, 2022)

[19] Amber Neely, Epic skirts Apple's 30% commission fee by implementing 'direct' payments, Apple Insider, (Aug, 13, 2020) available al https://appleinsider.com/articles/20/08/13/epic-skirts-apples-30-commission-fee-by-implementing-direct-payments (last visited April 17, 2022)

[20] Mike Peterson, Epic sues Apple after Fortnite removed from App Store, Aug. 13, 2020, available at https://appleinsider.com/articles/20/08/13/epic-sues-apple-after-fortnite-removed-from-app-store (last visited April 17, 2022)

[21] Id.

[22] Apple Insider Staff, Google follows Apple's lead, boots Fortnite from Play Store, Apple Inside, (August 14, 2020), available at https://appleinsider.com/articles/20/08/14/google-follows-apples-lead-boots-fortnite-from-play-store (last visited April 17, 2022)

[23] Sean Hollister, The Epic v. Google lawsuit finally makes sense, The Verge, (Aug 19, 2021) available at https://www.theverge.com/2021/8/19/22632804/epic-google-lawsuit-unredacted-complaint-antitrust (last visited April 17, 2022)

marketplace. Currently, the iPhone has a cost of anywhere from $500 to $1100, depending on the model and features selected.[24] The Android has a cost of $200 to $1200[25] and the PlayStation PS5 is estimated to be priced at $500-600 (with accessories).[26] And, unsurprisingly the apps and downloads do not work between or amongst systems, so the cost of switching is quite high and if not impossible due to proprietary formats and lack of data exporting features.

B. Privacy Destroying

Readers are undoubtedly aware that data collection, sharing, and hoarding is widespread in the digital ecosystem. For example, in 2021 the Federal Trade Commission (FTC) found (or verified) that many United States internet providers are collecting intimate personal data about their customers, and that customers are largely unaware of the scope and uninformed about their options for limiting this data collection. In fact:

> six internet providers that make up 98% of the US market are peeking in on customer's online activity, and sometimes engaging in worrying data practices: sharing information with third parties without customer knowledge or consent, logging real-time location data, and creating targeted advertising profiles among other issues.[27]

---

[24] iPhone 11 is $500 while the iPhone 13Pro is $1100. See Apple iPhone store https://www.apple.com/shop/buy-iphone/iphone-13-pro (last visited April 17, 2022)

[25] Android is the operating system, there is a wide range of phones that work on the Android system, so this is an estimate, based on AT&T service. See Android Store, available at https://www.att.com/buy/phones/browse/Android (last visited April 17, 2022). The most up to date information about the system can be found at the Android website, available at https://www.android.com/android-12/ (last visited April 17, 2022)

[26] PlayStation store, available at https://direct.playstation.com/en-us/ps5 (last visited April 17, 2022)

[27] Scott Ikeda, FTC Report on Data Collection: Internet Providers Quietly Harvesting Broad Range of Personal Information, Consumers Have Little Recourse, (Nov. 2, 2021) available at https://www.cpomagazine.com/data-privacy/ftc-report-on-data-collection-internet-providers-quietly-harvesting-broad-range-of-personal-information-consumers-have-little-recourse/ (last visited April 17, 2022) citing (full report) FTC Staff Report, A Look At What ISPs Know About You: Examining the Privacy Practices of Six Major Internet Service Providers, (Oct. 21, 2021) available at https://www.ftc.gov/system/files/documents/reports/look-what-isps-know-about-

And it's not a de minimis issue:

> Some appear to be intentionally deceptive and opaque in their data collection policies and promises to customers. "Several" of the internet providers publicly pledge to not sell customer data to third parties but do transfer it to their parent companies and affiliates or monetize it in other ways that don't involve a direct sale. "Many" provide consumers with only limited access to information about their stored personal data or present it in a confusing way. "Several" also use the contractual loophole of "business reasons" to store personal data indefinitely; they pledge to delete it after a certain period of time but can invoke vague "business reasons" to hold onto it beyond that.[28]

And, apps collect tons of data as well.[29] For example, in 2022 Jason Cohen in the PCMag article *These Apps Collect the Most Personal Data* notes: "Facebook, Instagram, and Messenger—all owned by the same company, Meta—collect all 32 segments of personal data that Apple's App Store flags."[30] While "If you're looking for privacy while searching the web, reading email, or streaming video, you should avoid Google's products."[31]

In 2014 an analysis of Android flashlight apps revealed that many of them require multiple permissions and gather user data with an attempt to later sell it.[32] The Android permission system allows the user to

---

you-examining-privacy-practices-six-major-internet-service-providers/p195402_isp_6b_staff_report.pdf (last visited April 17, 2022)

[28] Ikeda, FTC Report, supra, 27.

[29] Jason Cohen, These Apps Collect the Most Personal Data, PCMag, (Jan. 11, 2022) Available at https://www.pcmag.com/news/sick-of-data-collection-try-these-apps-instead (last visited April 17, 2022) Unfortunately, the information is not new. See Narseo Vallina-Rodriguez, Srikanth Sundaresan, 7 in 10 Smartphone Apps Share Your Data with Third-Party Services, Scientific America, (May 30, 2017), available at https://www.scientificamerican.com/article/7-in-10-smartphone-apps-share-your-data-with-third-party-services/ (last visited April 17, 2022).

[30] Cohen, These Apps Collect the Most Personal Data, supra 29.

[31] Cohen, These Apps Collect the Most Personal Data, supra 29.

[32] Joe Hindy, Are all flashlight apps really out to get you?, Android Authority, (dec. 9, 2014) available at https://www.androidauthority.com/are-all-flashlight-apps-

identify those spyware-like apps and restrict permissions, but essentially all the burden of monitoring and protecting one's privacy falls on the user and his or her technical abilities. Moreover, the default choices are most often set up not to the user's benefit and privacy protection.

However, a growing push seems to be occurring to begin to respect choice, autonomy, and privacy in the data driven online ecosystem. As Apple CEO Tim Cook stated:

> If a business is built on misleading users, on data exploitation, on choices that are no choices at all, then it does not deserve our praise. It deserves reform.
>
> We should not look away from the bigger picture. At a moment of rampant disinformation and conspiracy theories juiced by algorithms, we can no longer turn a blind eye to a theory of technology that says all engagement is good engagement—the longer the better—and all with the goal of collecting as much data as possible. Too many are still asking the question, "How much can we get away with?" when they need to be asking, "What are the consequences?"
> What are the consequences of prioritizing conspiracy theories and violent incitement simply because of their high rates of engagement? What are the consequences of not just tolerating, but rewarding content that undermines public trust in life-saving vaccinations? What are the consequences of seeing thousands of users join extremist groups, and then perpetuating an algorithm that

really-out-to-get-you-566448/ (last visited April 17, 2022). Of course, this also implicates the notice and consent model, which has been widely criticized, for years by many. Most recently, the FTC Chair Lina Khan suggested "a shift away from the "outdated and insufficient" notice and consent framework, where companies ask consumers to agree to lengthy privacy policies that are heavy on legal text. " Andrea Vittorio , FTC Chair Calls for Shift From 'Overwhelming' Privacy Policies, Bloomberg Law, (April 11, 2022) available at https://news.bloomberglaw.com/privacy-and-data-security/ftc-chair-calls-for-shift-from-overwhelming-privacy-policies#:~:text=The%20Federal%20Trade%20Commission's%20leader,and%20use%20of%20consumer%20data. (last visited April 17, 2022).

> recommends even more?
> It is long past time to stop pretending that this approach doesn't come with a cost—of polarization, of lost trust and, yes, of violence. A social dilemma cannot be allowed to become a social catastrophe. [33]

And it seems the privacy activity, especially in primary access devices can make a difference. For example, in April 2021 when Apple released iOS 14.5[34] it began enforcing a policy called App Tracking Transparency.[35] iPhone, iPad, and Apple TV apps are now required to request users' permission to use techniques like IDFA (ID for Advertisers) to track those users' activity across multiple apps for data collection and ad targeting purposes. [36]

The *Financial Times* found that most users have opted out of tracking using Apple's App Tracking Transparency (ATT) framework,[37] a requirement that forces developers to ask users if they wish to be tracked across other apps and websites.[38] Data in the report from Lotame, a third-party company, suggests that Meta, YouTube, Twitter, and Snap

---

[33] Samuel Axon, Everything that happened in Apple and Facebook's privacy feud today, ArsTechnica, (Jan, 28, 2021) available at https://arstechnica.com/gadgets/2021/01/why-facebook-and-apple-are-going-to-war-over-privacy/ (last visited April 17, 2022).

[34] Samuel Axon, Apple releases iOS 14.5, the biggest update since iOS 14 first launched, ArsTechnica (April 26, 2021) https://arstechnica.com/gadgets/2021/04/apple-releases-ios-14-5-the-biggest-update-since-ios-14-first-launched/ (last visited April 17, 2022).

[35] See id. This was not the first- or only- time Apple took a stand in this area. See Anmol Sachdeva,
Apple Restricts App Developers From Sharing Users' Contacts And Other Data, FossBytes, (June 13, 2018) https://fossbytes.com/apple-restricts-app-developers-from-sharing-users-contacts-and-other-data (last visited April 17, 2022).

[36] Axon, Apple releases iOS 14.5, the biggest update, supra note 34. For the full policy see Apple Store, Developer User Privacy available at https://developer.apple.com/app-store/user-privacy-and-data-use/ (last visited April 17, 2022).

[37] Samuel Axon, 96% of US users opt out of app tracking in iOS 14.5, analytics find, ArsTechnica (May 7, 2021) available at https://arstechnica.com/gadgets/2021/05/96-of-us-users-opt-out-of-app-tracking-in-ios-14-5-analytics-find/ (last visited April 17, 2022).

[38] Sami Fathi, Apple's Privacy Features Have Cost Social Media Companies Nearly $10 Billion in Revenue, Mac rumors, (Nov. 1, 2021) available at https://www.macrumors.com/2021/11/01/apple-privacy-social-media-companies/ (last visited April 17, 2022).

lost $9.85 billion in revenue in the third and fourth quarters of 2021.[39]

Meta's stock prices plunged after the company reported that Apple's privacy features would cost it billions this year.[40] As a result, as Eric Seufert, a media strategist and author of Mobile Dev Memo, a blog about mobile advertising "[p]eople can't really be targeted the way they were before."[41]. . . "That breaks the model. It's not just an inconvenience that can be fixed with a couple of tweaks. It requires rebuilding the foundation of the business."[42]

C. Purchase Decisions Made on a Privacy Promise

A quick glance at the Android 12 platform description shows an effort to focus on the privacy aspects of the platform. For example, Android 12 description includes 'Private by design, so you are in control."[43] Which is then described as "Android 12 is designed for your safety. With new easy-to-use, powerful privacy features, you'll have peace of mind knowing that you have control over who can see your data and when."[44] In fact, as you open the Android 12 webpage, there are three key aspects: personal, safe, and effortless.[45] Privacy has clearly become a selling point.

Of course, the Android operating system is not alone in emphasizing privacy - and control over data and sharing as a key feature of the newest operating systems. As described above, Apple was an early mover in emphasizing privacy, including creating individual controls over data sharing. However, as described in more details below, those

---

[39] See id.

[40] Kate Conger and Brian X. Chen, A Change by Apple Is Tormenting Internet Companies, Especially Meta, New York Times, (Feb, 3, 2022) available at https://www-nytimes-com.cdn.ampproject.org/c/s/www.nytimes.com/2022/02/03/technology/apple-privacy-changes-meta.amp.html (last visited April 17, 2022).

[41] https://mobiledevmemo.com/ (last visited April 17, 2022); see Sami Fathi, Apple's Privacy Rules to Blame for Facebook's Lower Than Expected Quarterly Growth, Says Zuckerberg, Mac Rumors (Oct. 26, 2021) available at https://www.macrumors.com/2021/10/26/apple-privacy-rules-blame-facebook-earnings/ (last visited April 17, 2022).

[42] https://mobiledevmemo.com/ (last visited April 17, 2022).

[43] Android website, Android 12 information, available https://www.android.com/android-12/ (last visited April 17, 2022).

[44] See id.

[45] See id.

controls may not be as they seem.

D. Selectively Uphold the Terms of Participating the in the Marketplace

Do keep in mind, Apple does in fact- limit, restrict and/or comply with local laws- when it serves its purpose. For example, Apple willingly complies with Chinese laws that restrict users' access to thousands of apps and that require foreign companies to store the data of its citizens within the country and make them available to authorities.[46] In contrast, Google has gone further to resist such Chinese pressure.[47]

Apple has also censored news platforms such as *The New York Times* and Bloomberg News- in China,[48] while in Hong Kong it blocked the access to the HK Maps app that supported the local democracy protests.[49] It has also agreed to delete dozens of apps, including podcasts, that China says violate local censorship laws.[50]

Moreover, Apple has removed or restricted applications, for various reasons, in the past. For example, in 2019 Apple removed or restricted some third-party screen time and parental control apps[51] because

> the apps violated its rules, that third-party apps could gather too much data on devices, and that the actions weren't related to the company's debut of its own screen-monitoring tools.[52]

---

[46] Masha Borak, Apple removed 805 apps in China from 2018 to 2019, Abacus, (Jan, 29, 2020) available at https://www.scmp.com/abacus/tech/article/3048047/apple-removed-805-apps-china-2018-2019 (last visited April 17, 2022).

[47] BBC Author, China condemns decision by Google to lift censorship , BBC News, (March 23, 2010) available at http://news.bbc.co.uk/2/hi/asia-pacific/8582233.stm (last visited April 17, 2022).

[48] Andy Yen, Freedom is a human right, and we are committed to defending it even when others won't Proton Mail, (Oct. 21, 2019) available at https://protonmail.com/blog/protesters-free-speech/ (last visited April 17, 2022).

[49] See id.

[50] See id.

[51] Andrew Liptak, Apple explains why it's cracking down on third-party screen time and parental control apps, The Verge (April 4, 2019) available at https://www.theverge.com/2019/4/27/18519888/apple-screen-time-app-tracking-parental-controls-report (last visited April 17, 2022).

[52] See id.

And, of course in 2020 Epic Games Inc. accused Apple Inc. of threatening to block it from making software for iOS devices and Mac computers.[53] Epic Games is not alone, in fact other app developers have experienced similar issues with Apple and Google over their marketplace policies, including Netflix Inc. and Spotify Technology SA.[54]

In February 2022, Google announced it would begin to restrict apps from tracking you on Android devices.[55] This was in response to the long-standing push back Google was receiving from privacy advocates and others as:

> Google includes a unique identifier on Android devices, called Advertising ID, that allows marketers to see what a user is doing across all apps, allowing companies to build a comprehensive picture of that person's interests and activities.[56]

Of course, the February announcement is an attempt to "raise the bar for user privacy"[57] by limiting (but not preventing) apps' ability to capture that information. Yet, one does not have to look far for research that pokes holes in the promise. For example, in April of 2022, Konrad Kollnig and others published a paper entitled *Goodbye Tracking? Impact of iOS App Tracking Transparency and Privacy Labels*[58] in which they assert:

---

[53] Sarah E. Needleman, Fortnite' Creator Says Apple Is Threatening to Curb Access to Software Tools -- 3rd Update, Investors Hub, (Aug. 17, 2020) available at https://ih.advfn.com/stock-market/NASDAQ/apple-AAPL/stock-news/83088656/fortnite-creator-says-apple-is-threatening-to-curb (last visited April 17, 2022).

[54] See id.

[55] Irina Ivanova, Google to restrict apps from tracking you on Android devices, CBS News, (Feb, 16, 2022) available at https://www.cbsnews.com/news/android-tracking-google-limits/ (last visited April 17, 2022).

[56] See id.

[57] See id.

[58] Konrad Kollnig, Anastasia Shuba, Max Van Kleek, Reuben Binns, Nigel Shadbolt, Goodbye Tracking? Impact of iOS App Tracking Transparency and Privacy Labels, re-print of paper that has been accepted for publication by the ACM Conference on Fairness, Accountability, and Transparency (FAccT) 2022, available at https://arxiv.org/abs/2204.03556 (last visited April 17, 2022).

> We find that Apple's new policies, as promised, prevent the collection of the Identifier for Advertisers (IDFA), an identifier used to facilitate cross-app user tracking. However, many apps still collect device information that can be used to track users at a group level (cohort tracking) or identify individuals probabilistically (fingerprinting). We find real-world evidence of apps computing and agreeing on a fingerprinting-derived identifier through the use of server-side code, thereby violating Apple's policies and exposing the limits of what ATT can do against tracking on iOS. This is especially concerning because we explicitly refused opt-in to tracking in our study, and consent is a legal requirement for tracking under EU and UK data protection law. We find that Apple itself engages in some forms of tracking and exempts invasive data practices like first-party tracking and credit scoring from its new rules, and that the new Privacy Nutrition Labels were often inaccurate.[59]

They continue:

> Overall, our findings suggest that, while tracking individual users is more difficult now, the changes reinforce existing market power of gatekeeper companies with access to large troves of first-party data. [60]

It may be an ecosystem that demands loyalty to the platform, destroys privacy, misleads, or otherwise intentionally subverts the acquisition of knowledge needed to make a reasonable choice about the way the environment behaves, and selectively enforces terms- those users of the app ecosystem assume are part of the protections within the environment, might benefit- strongly, from external monitoring and enforcement.

---

[59] See id.
[60] See id.

III. OSTROM GOVERNANCE AS A KEY CONSIDERATION

In the context of this type of technology marketplace, many different aspects of rules and behavioral intervention must work together to build a governance ecosystem. Many argue, no technology regulation can occur alone. Instead, we must improve individual literacy, insist upon technology driven intervention and regulate how that intervention occurs, while consequences those that fail to comply. To date, few technology marketplaces have undergone such a level of attention to building a governance ecosystem. To move forward, such a governance system must begin to emerge. A reasonable first step, monitoring, and enforcement- as one important key.

A. The Importance of Monitoring and Enforcement

Despite all the current conversation and promises by various marketplace hosts to focus on privacy, there is little requiring the hosts to abide by the self-imposed rules. Moreover, the self-imposed rules are easy to change, simple to not enforce, and there are no real consequences for any of these activities. For example, it is now widely known that between April 22, 2010, and Sept. 26, 2011, Facebook users in the United States were tracked even after they logged out of the social media website.[61]

Yet, this is not an article *about* Facebook, this is about the various marketplaces, promising to uphold limited tracking as a rule of participating in the marketplace- yet, not removing or otherwise restricting Facebook from the app marketplace. And, no reader will be unfamiliar with the Cambridge Analytica in which the personal data of up to 87 million[62] Facebook users were acquired via the 270,000 Facebook users who used a Facebook app called "This Is Your Digital Life."[63] By

---

[61] Jonathan Stempel, Meta's Facebook to pay $90 million to settle privacy lawsuit over user tracking, Reuters, (Feb. 15, 2022) available at https://www.reuters.com/technology/metas-facebook-pay-90-million-settle-privacy-lawsuit-over-user-tracking-2022-02-15/ (last visited April 17, 2022).

[62] Cecilia Kang, Sheera Frenkel, Facebook Says Cambridge Analytica Harvested Data of Up to 87 Million Users, New York Times, (April 4, 2018) available at https://www.nytimes.com/2018/04/04/technology/mark-zuckerberg-testify-congress.html (last visited April 17, 2022).

[63] Alex Hern, How to check whether Facebook shared your data with Cambridge Analytica, The Guardian, (April 10, 2018) Available at

giving this third-party app permission to acquire their data, back in 2015, this also gave the app access to information on the user's friends network; this resulted in the data of about 87 million users, the majority of whom had not explicitly given Cambridge Analytica permission to access their data, being collected.[64] Of course, the app developer breached Facebook's terms of service by giving the data to Cambridge Analytica; yet, few speak of the fact that Facebook's failure to ensure data sharing was occurring as proscribed in the App Marketplace ToS was also a major issue- in which no action was truly taken by any of the app marketplaces. Even after the US Federal Trade Commission announced it is "conducting an open investigation of Facebook Inc's privacy practices. . ."[65] and Facebook acknowledged the concerns of improper data handling.[66] Despite these astonishing breaches of trust, the app marketplace took no real action. And, of course, there is growing evidence that the issues- despite the 2019 settlement related to the Cambridge Analytica scandal,[67] has not really resulted in a true level of privacy robustness as Brave decided to block the installation of a popular Chrome extension called L.O.C. because it exposes users' Facebook data to potential theft.[68] In this situation, it is alleged that

---

https://www.theguardian.com/technology/2018/apr/10/facebook-notify-users-data-harvested-cambridge-analytica (last visited April 17, 2022).

[64] Kurt Wagner, Here's how Facebook allowed Cambridge Analytica to get data for 50 million users, Vox Recode, (March 17, 2018) available at https://www.vox.com/2018/3/17/17134072/facebook-cambridge-analytica-trump-explained-user-data (last visited April 17, 2022).

[65] Reuters Author, U.S. FTC investigating Facebook's privacy practices, Reuters, (March 26, 2018) Available at https://news.trust.org/item/20180326145505-6je9o/ . (last visited April 17, 2022). If the FTC finds Facebook violated terms of the consent decree, it has the power to fine the company thousands of dollars a day per violation, which could add up to billions of dollars. (See id.)

"The FTC takes very seriously recent press reports raising substantial concerns about the privacy practices of Facebook. Today, the FTC is confirming that it has an open non-public investigation into these practices," (Id.)

[66] Wong, Julia Carrie, Facebook acknowledges concerns over Cambridge Analytica emerged earlier than reported, *The Guardian.* (March 22, 2019) available at https://www.theguardian.com/uk-news/2019/mar/21/facebook-knew-of-cambridge-analytica-data-misuse-earlier-than-reported-court-filing (last visited April 17, 2022).

[67] Colin Stretch. FTC Agreement Brings Rigorous New Standards for Protecting Your Privacy, Meta, July 24, 2019) available at https://about.fb.com/news/2019/07/ftc-agreement/ (last visited April 17, 2022).

[68] Thomas Claburn, Facebook is one bad Chrome extension away from another Cambridge Analytica scandal, The Register, (Feb. 17, 2022) available at https://www.theregister.com/2022/02/17/chrome_meta_token/ (last visited April 17, 2022).

Facebook exposes 'god mode' tokens that could be used to siphon data.[69] (Will any of the app marketplaces take action in the face of another egregious Facebook privacy issue)

As Nobel laureate Elinor Ostrom emphasized, credible commitment and monitoring are essential to creating durable rules. Further, the importance of enforcement in shaping whether people will consider a rule to be "real" and worth following is one of the reasons why fieldwork was so important for the Ostroms.[70] For example,

> In her examination of the rules of property use within a community, Elinor distinguished between rules in use and rules in form, and we would like to stress as well the function, or reason, of rules. What matters for human conduct are the rules in use as that is where the functional significance of any rule is determined. In many circumstances, the rules in use are at odds with the rules in form that are formally adopted. When the formal rules are either not enforced or in conflict with the informal rules in use, social intercourse is plagued with social tensions and ambiguities. These will either be worked out in specified contexts, or the lack of enforcement will result in social conflict.[71]

Moreover, for a rule to be stable over the long term, the belief that a rule will be enforced will likely need to be substantiated by an actual predictable enforcement process and a belief in the legitimacy of that process. Sorting out the real rules from the fake requires being on the ground and observing actual behavior and enforcement practices.[72]

B.. Why Trust and Trustworthiness Matter

As readers have undoubtedly noticed, much of the conversation

---

[69] Facebook exposes 'god mode' token that could siphon data, The Register, (Feb 12, 2022) available at https://www.theregister.com/2022/02/12/facebook_god_mode/ (last visited April 17, 2022).

[70] Peter Boettke, Jayme Lemke, and Liya Palagashvili, Riding in Cars with Boys: Elinor Ostrom's Adventures with the Police, Journal of Institutional Economics 9 (4): 407–25. (2013).

[71] See id.

[72] See id.

surrounding the data, privacy and data within the marketplace driven environment has evolved from security and trust, and moving into a 'trustworthy; driven narrative. This is because the concept of trust (*i.e.* a firm belief in the integrity, ability, or character of a person or thing; confidence or reliance.) demands an evaluation of the actions. Trustworthiness likely gives us the measure necessary to make a determination of trust. For example, the National Artificial Intelligence Initiative Office (within the White House Office of Science and Technology Policy (OSTP)) notes:

> To be trustworthy, AI technologies must appropriately reflect characteristics such as accuracy, explainability and interpretability, privacy, reliability, robustness, safety, and security or resilience to attacks – and ensure that bias is mitigated. Factors such as fairness and transparency should be considered, particularly during deployment or use. In addition, the broader impacts of AI on society must be considered, such as implications for the workforce. Developing and using AI in ways that are ethical, reduce bias, promote fairness, and protect privacy is essential for fostering a positive effect on society consistent with core U.S. values.[73]

Trustworthiness encompasses and has a more specific, granular, defined set of expectations of measures and values that need to be considered and as such, the authors suggest the robustness of trustworthiness will serve the conversation better, moving forward. It is likely however the case, that the more an entity meets the standards established to be trustworthy, the individual is more justified to trust the entity. And of course, research in this area leads the authors to argue that this is the key reason that misinformation, hidden terms, poor behavior, and similar negative behaviors are essential considerations in these environments. 'Hidden' activity and nudges eliminate or reduce an individual's ability to evaluate trustworthiness- and thus, any trust placed in the entity is in fact likely to be misplaced! But it is difficult to hold the individual responsible for that misplaced trust- and they lacked the information to evaluate trustworthiness of the entity.

---

[73] National Artificial Intelligence Initiative Office (NAIIO), Advancing Trustworthy AI website available at https://www.ai.gov/strategic-pillars/advancing-trustworthy-ai/ (last visited April 17, 2022).

IV. A POSSIBLE WAY FORWARD

One wonders the impact of some of the most recent initiatives to restrict or otherwise regulate data within the Big Tech Controlled data ecosystem, As people are likely aware in February 2022 the Senate Judiciary Committee Approves Antitrust Bill Targeting Big Tech. Senate Bill 2710[74] addresses Apple and Google in particular, who oversee the Apple App Store and the Google Play Store, which together mediate access to the vast majority of apps used by smartphone users.[75] In general, the legislation is seen as an "attempt to curtail the power of the two major app store providers, who have a long history of using their domination of the market to exert power over information, content, and capital on the internet."[76]

Yet, many feel too little is being done to curtail widespread abuse of consumer trust. In March of 2022, Rohit Chopra of the Consumer Financial Protection Bureau in his Distinguished Lecture on Regulation at the University of Pennsylvania Law School entitled Reining in Repeat Offenders[77] highlighted a key question as we move forward:

> How do we stop large dominant firms from violating the law over and over again with seeming impunity? Corporate recidivism has become normalized and calculated as the cost of doing business; the result is a rinse-repeat cycle that dilutes legal standards and undermines the promise of the financial sector and the entire market system.[78]

---

[74] S.2710 - Open App Markets Act117th Congress (2021-2022) |information available at https://www.congress.gov/bill/117th-congress/senate-bill/2710?s=1&r=23 (last visited April 17, 2022).

[75] Nicholas Dolinger, Senate Judiciary Committee Approves Antitrust Bill Targeting Big Tech, The Epoch times, (Feb. 3, 2022) available at https://www.theepochtimes.com/senate-judiciary-committee-approves-antitrust-bill-targeting-big-tech_4255616.html (last visited April 17, 2022).

[76] See id.

[77] Rohit Chopra, 2022 Distinguished Lecture on Regulation, University of Pennsylvania Law School entitled Reining in Repeat Offenders (March 2022) available at https://www.consumerfinance.gov/about-us/newsroom/reining-in-repeat-offenders-2022-distinguished-lecture-on-regulation-university-of-pennsylvania-law-school/ (last visited April 17, 2022).

[78] Id

He goes on to note:

> We must forcefully address repeat lawbreakers to alter company behavior and ensure companies realize it is cheaper, and better for their bottom line, to obey the law than to break it.[79]

Of course, his focus is very much on the large financial institutions, such as Citigroup, JPMorgan Chase, Wells Fargo, American Express, and Discover.[80] But he turns his attention to an entity well known to anyone, Facebook.[81] He notes:

> I now want to discuss one of the best examples of failed repeat offender enforcement: the Federal Trade Commission's treatment of one of the largest and most well-known corporations in the world: Facebook. Facebook is a clear example of a politically powerful firm that routinely violated the terms of its government order with no real consequences.

It is important to note, Rohit Chopra was the FTC Commissioner from May 2, 2018, until October 12, 2021.[82] Thus, the next comments are particularly noteworthy.

> The agency was in deep decay and disarray after years of lax enforcement against large corporate actors,

---

[79] Id

[80] Id.

[81] He notes, this is a reasonable and appropriate consideration, noting:

I raise Facebook not only because it is such an egregious case but also because of the potential of very large firms entering financial services. It's clear that Big Tech wants to get into the market, as we saw with Facebook's failed attempt to create a new global currency. We've also seen Alibaba, Amazon, Google, and Tencent *entering financial services, including with payments, money management, insurance, and lending*. Given their size and customer reach, their entry has the potential to transform the industry. How these companies engage in other business practices is how we can expect them to engage in financial services, so it is worth going into some detail about the FTC case against one of the biggest players in this space.
Chopra, 2022 Reining in Repeat Offenders, supra note 77

[82] Chopra, 2022 Reining in Repeat Offenders, supra note 77

> spanning multiple administrations. In some of the most widespread recent nationwide crises, from the 2008 financial disaster to the opioid epidemic to the student loan and for-profit college scandals, the FTC was essentially missing. On a bipartisan basis, the Commission heavily relied on a "no-money, no-fault" settlement strategy, where wrongdoers essentially faced no consequences, even in cases of egregious fraud.[83]

His comments are particularly noteworthy, as they are a clear signal that the FTC, at the time, was incapable of enforcement. As noted above, when formal rules are not enforced social intercourse is plagued with social tensions and ambiguities.[84]

Yet, according to former FTC Commissioner Chopra the absence of enforcement is not the end of the conversation, in fact, the events are significantly more troubling, as: "It was clear to many that the company [Facebook] paid off the FTC to minimize scrutiny of its top executives' role in the order violations."[85]

Now, the Director of the Consumer Financial Protection Bureau, Director Chopra states:

> Achieving general deterrence is an important goal for the CFPB. We need penalties where the expected financial benefits of an illegal scheme do not outweigh the expected costs. And we need an understanding that agency and court orders are not suggestions.[86]

He goes on:

> Put plainly, regulators charged with overseeing large institutions have lost credibility when it comes to halting repeat offenders. While headline-driven penalties give the guise of deterrence, they do not work for

---

[83] Chopra, 2022 Reining in Repeat Offenders, supra note 77
[84] Boettke, Riding in Cars with Boys, supra note 70.
[85] Chopra, 2022 Reining in Repeat Offenders, supra note 77
[86] Id.

dominant, powerful firms.[87]

Fortunately, the FTC may have found one mechanism of enforcement, algorithmic destruction.[88] In a March 4 settlement order,[89] the agency demanded that WW International[90] destroy the algorithms and/or AI models it built using personal information collected from kids as young as 8 without parental permission.[91] The agency also fined the company $1.5 million and ordered it to delete the illegally harvested data.[92]

Moreover, the Securities and Exchange Commission has also entered the arena more actively. For example, in February a pair of whistleblower complaints allege Facebook misled investors about its efforts to combat climate change and covid-19 misinformation.[93] The complaints allege that the company made "material misrepresentations and omissions in statements to investors" about its efforts to combat misinformation.[94]

Of course, the FTC, SEC, and the Consumer Financial Protection Bureau all becoming more active in addressing the misplaced trust of consumers in the online world is an important step in the right direction toward turning the tide of consumer trust. As Director Chopra states:

> In the end, large dominant firms should be subject to the same consequences of enforcement actions as small firms. We need to end double-standard enforcement that exists. We need to move away from just monetary penalties and consider an arsenal of options that really

---

[87] Id.

[88] Kate Kaye, The FTC's new enforcement weapon spells death for algorithms, Protocol, (March 14, 2022), available at https://www.protocol.com/policy/ftc-algorithm-destroy-data-privacy (last visited April 17, 2022).

[89] Ben Brody, Weight Watchers must delete algorithms built from kids' data, Protocol, (march 4, 2022)(available al https://www.protocol.com/bulletins/weight-watchers-coppa-ftc (last visited April 17, 2022).

[90] Formerly known as Weight Watchers. See id.

[91] Kaye, FTC New Enforcement, supra note 88.

[92] See id.

[93] Cat Zakrzewsk, Facebook whistleblower alleges executives misled investors about climate, covid hoaxes in new SEC complaint, The Washington Post, (Feb. 18, 2022) available at https://www.washingtonpost.com/technology/2022/02/18/whistleblower-facebook-sec-climate-change/ (last visited April 17, 2022).

[94] Id.

> work to stop repeat offenses.[95]

However, it is important to note, more can be done to protect consumers and return trust into a business model that seems to be designed to mislead, deceive, and manipulate consumers. Again, as Director Chopra notes:

> More importantly, when the public perceives those powerful actors in the economy and society live by a different set of rules, this deeply undermines the promise of the rule of law and our market system. We can and must change course on this.[96]

How might this type of regulatory environment be accomplished:

1. Federal entities must be empowered and funded to protect consumers in the way envisioned by the agency mandate
2. Consumers need the right to insist terms of service and other agreements are enforced.
3. Entities that control digital marketplaces must be required to enforce their terms of participation in the marketplace.
4. Entities that control digital marketplaces must be required to monitor their marketplace for compliance with the terms of participating in the marketplace.
5. Entities that control digital marketplaces must be required to enforce their terms of participating in the marketplace, across all marketplace actors.
6. Entities that control digital marketplaces must provide true notice of change in terms of service, which must include change of terms related to data sharing agreements regardless of if that data sharing is deemed internal or external (third party sharing)
7. The federal government should immediately consider building an federal agency such as the Consumer Financial Protection Bureau, that has a similar mandate but includes digital environments, not merely focused on financial

---

[95] Chopra, 2022 Reining in Repeat Offenders, supra note 77
[96] Id.

products.[97]

Of course, this list is the regulatory aspects of a much larger question, with an incredibly complex response required. As briefly highlighted in the paper, individuals must begin to be more literate in the use of technology. Yet, regulation must ensure people are not targeted for misleading and deceptive activities that make the best of literacy programs useless. Of course, industry itself can begin to embrace privacy and trustworthiness- yet, transparency, monitoring and accountability is one of the only ways to ensure individual and society trust is not misplaced. And, the industry and others, including various governmental agencies, can build mechanisms to monitor, even aspects of the system that are difficult for most to observe, yet in many ways we all may need to give up a little piece of privacy to allow some of that to happen. This paper is certainly not an attempt to solve all the problems in a complex ecosystem of governance needs. Several things are however clear: (1) the time of blindly trusting those that self-regulate must end; (2) governmental agencies must be empowered to act and must be held to a standard that demands action, and (3) much more needs to be done, including (most likely) an agency with the skills and focus placed upon our digital world.

V. CONCLUSION

As can be seen from the examples in this paper, there are any number of issues that arise when a consumer decides to enter- and remains captured- in one of the app marketplaces. Outside the world of antitrust however, the arguments being advanced in this paper is that the narratives that are made to encourage and influence an individual to select

---

[97] One wonders what will happen with the new State Department Bureau of Cyberspace and Digital Policy that is specifically mandated to:

leads and coordinates the Department's work on cyberspace and digital diplomacy to encourage responsible state behavior in cyberspace and advance policies that protect the integrity and security of the infrastructure of the Internet, serve U.S. interests, promote competitiveness, and uphold democratic values.

U.S. Department of State, Bureau of Cyberspace and Digital Policy, Website, available at https://www.state.gov/bureaus-offices/deputy-secretary-of-state/bureau-of-cyberspace-and-digital-policy/ (last visited April 17, 2022).

a particular marketplace must certainly include recognition of the growing commitment to privacy and protection. In these instances, it is reasonable to assume that the decision to become beholden to the marketplace is at least partially determined based on messaging of a commitment of trust and trustworthiness. As such, the marketplace gatekeepers should be held to these promises.