

Lomborg, Stine; Sick, Kristian; Flensburg, Sofie; Lai, Signe Sophus

## Article

# Monitoring infrastructural power: Methodological challenges in studying mobile infrastructures for datafication

Internet Policy Review

## Provided in Cooperation with:

Alexander von Humboldt Institute for Internet and Society (HIIG), Berlin

*Suggested Citation:* Lomborg, Stine; Sick, Kristian; Flensburg, Sofie; Lai, Signe Sophus (2024) : Monitoring infrastructural power: Methodological challenges in studying mobile infrastructures for datafication, Internet Policy Review, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 13, Iss. 2, pp. 1-28, <https://doi.org/10.14763/2024.2.1763>

This Version is available at:

<https://hdl.handle.net/10419/300739>

## Standard-Nutzungsbedingungen:

Die Dokumente auf EconStor dürfen zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden.

Sie dürfen die Dokumente nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, öffentlich zugänglich machen, vertreiben oder anderweitig nutzen.

Sofern die Verfasser die Dokumente unter Open-Content-Lizenzen (insbesondere CC-Lizenzen) zur Verfügung gestellt haben sollten, gelten abweichend von diesen Nutzungsbedingungen die in der dort genannten Lizenz gewährten Nutzungsrechte.

## Terms of use:

*Documents in EconStor may be saved and copied for your personal and scholarly purposes.*

*You are not to copy documents for public or commercial purposes, to exhibit the documents publicly, to make them publicly available on the internet, or to distribute or otherwise use the documents in public.*

*If the documents have been made available under an Open Content Licence (especially Creative Commons Licences), you may exercise further usage rights as specified in the indicated licence.*



<https://creativecommons.org/licenses/by/3.0/de/legalcode>



RESEARCH  
ARTICLE



OPEN  
ACCESS



PEER  
REVIEWED

# Monitoring infrastructural power: Methodological challenges in studying mobile infrastructures for datafication

**Stine Lomborg** *University of Copenhagen*

**Kristian Sick** *University of Copenhagen*

**Sofie Flensburg** *University of Copenhagen*

**Signe Sophus Lai** *University of Copenhagen*

**DOI:** <https://doi.org/10.14763/2024.2.1763>

**Published:** 26 June 2024

**Received:** 30 October 2023 **Accepted:** 8 March 2024

**Funding:** The research for this article was part of the Datafied Living project, funded by the ERC Grant No. 947735.

**Competing Interests:** The author has declared that no competing interests exist that have influenced the text.

**Licence:** This is an open-access article distributed under the terms of the Creative Commons Attribution 3.0 License (Germany) which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. <https://creativecommons.org/licenses/by/3.0/de/deed.en>  
Copyright remains with the author(s).

**Citation:** Lomborg, S. & Sick, K. & Flensburg, S. & Sophus Lai, S. (2024). Monitoring infrastructural power: Methodological challenges in studying mobile infrastructures for datafication. *Internet Policy Review*, 13(2). <https://doi.org/10.14763/2024.2.1763>

**Keywords:** Infrastructure, Mobile apps, Software development kit (SDK), Datafication, Infrastructural power

**Abstract:** This article discusses how we can locate and understand infrastructural power in mobile infrastructures for datafication through dissecting third-party tracking via so-called software development kits (SDKs). As key material components of mobile infrastructures, SDKs enable app functionality, security, and access to data collection and use by third-party services. However, the methods for investigating SDKs and mobile datafication in general are fragile and in urgent need of development and critical discussion. We explore and discuss methodological pathways for understanding power in the mobile ecosystem. Through exemplifying empirical interventions, derived from a sample of 1129 apps used by 69 Danes participating in the Datafied Living research project, we investigate and discuss how Apple and Alphabet hold infrastructural power and perpetually consolidate their effective mobile duopoly while simultaneously protecting and enhancing their assets in related data markets (e.g. through mobile advertising). We argue that the current infrastructures for mobile datafication impede transparency, systematic democratic monitoring, and ultimately regulation while also limiting the critical capabilities of researchers, as well as open source and hacker environments who must constantly adjust their counter-intelligence measures and tools.

This paper is part of **Locating and theorising platform power**, a special issue of *Internet Policy Review* guest-edited by David Nieborg, Thomas Poell, Robyn Caplan and José van Dijck.

## Introduction

In early 2022, the Austrian Data Protection Authority announced a landmark decision concerning the use of the (in)famous web tracking tool, Google Analytics (noyb, 2022). Stating that it violated the EU's General Data Protection Regulation (GDPR) by collecting and transferring users' personal data to the US, the Austrian decision provoked similar discussions in other European countries (see e.g. EDPB, 2022; Datatilsynet, 2022). These rulings mark a moment of change in European data regulation and testify to how regulation can impact the market of third-party tracking. However, they also indicate the need for systematic monitoring and control of the broader ecosystems of third-party tracking to ensure the enforcement of new legislative frameworks. Before the rulings, Google Analytics was the de facto standard tool for web traffic analysis. Now it has largely disappeared, but the tracking and analytics features that Google Analytics embedded are now part of similar third-party services across web and mobile infrastructures, including Google's own Firebase Analytics.

Looking beyond the specific example of Google Analytics, third-party services constitute a key component of contemporary data infrastructures by supplying the technical tools used by websites and mobile apps to, for instance, collect, store and process user data, serve ads, detect crashes, and much more (Binns et al., 2018; Lai & Flensburg, 2021). Creeping into all aspects of mundane, datafied living, these services shape the underlying conditions for an ever-growing range of everyday activities and thereby comprise a critical part of contemporary digital societies. By continuously improving and introducing new tools and services while also acquiring new businesses and their products, actors such as Google (Alphabet) extend their digital empires beyond their own websites and mobile apps, thereby amplifying what has been referred to as processes of platformization (Helmond, 2015; Nieborg & Poell, 2018; Poell et al., 2019) and infrastructuralisation, i.e. the process of platforms becoming or co-existing with infrastructures used in daily life (Plantin et al., 2018).

Despite the recent backlash against specific third-party services such as Google Analytics, the market for supplying them has largely managed to stay under the radar of official monitoring initiatives and democratic intervention. The cases men-

tioned above are all based on individual case and company-specific complaints, as regulatory efforts tend to focus on individual companies and services rather than on the market at large. While legislative frameworks have been developed to target so-called cookies that are generated on websites (which is also the focus of the cases against Google Analytics), systematic monitoring and market analyses are not performed or released by public authorities on either an EU or nation state level.

In the ever-growing market for mobile apps – and tracking – monitoring initiatives and regulatory interventions are even more scarce. Since third-party services in mobile app environments operate quite differently from their predecessors in the web market, researchers and regulators must develop new methods for detecting them. This is because when studying and regulating third-party tracking across digital systems, we are dealing with a moving target that evolves at a faster pace than legislative processes can keep up with. The rulings mentioned above thereby also draw attention to important limitations in the current approach to third-party regulation that tend to focus on specific platforms and web-based tracking rather than the broader tracking market and post-cookie technologies. If we are to address these gaps and create a foundation for more effective monitoring and regulation of the data market, we – as researchers, regulators, and the public in general – need to pay attention to the technical underpinnings of platformisation and their consequences for the distribution of power.

In this article, we follow recent calls for addressing “public accountability issues at the ‘root’ level of the communication infrastructure” (Mansell & Plantin, 2022, p. 2) by approaching third-party services as key entry points for studying contemporary infrastructural power (Mann, 1984). As a companion to platform power (van Dijck et al., 2019), the notion of infrastructural power emphasises the ways simple technical procedures and changes to system architecture may effectively alter market dynamics and, by extension, political-economic power relations in digital communication systems (Lomborg et al., 2023). If we are to address, critically discuss, and ultimately regulate digital communication systems and data markets, we need better insight into, and solid methods for assessing, the commercial and infrastructural activities within them, and how such activities are embedded in the material fabric of mundane digital communication.

In particular, we discuss how to locate and understand infrastructural power in mobile infrastructures for datafication through dissecting third-party tracking via so-called software development kits (SDKs) (Gerlitz et al., 2019; Kollnig et al. 2021). Focusing on the largest suppliers of mobile operating systems and app

stores, we explore the conditions for studying and monitoring third-party tracking in ecosystems controlled by two tech giants: Apple (iOS and App Store) and Alphabet (Android and Google Play Store). We provide empirical examples from a subsample of five prominent apps for Danish welfare provision derived from a dataset consisting of a total of 1,129 apps used by 69 Danes to illustrate the practical and epistemic implications of big tech's control of the mobile app environment. These explorations show how Apple and Alphabet design their respective mobile infrastructures in ways that consolidate their effective duopoly in the mobile market while simultaneously protecting and enhancing their assets in related data markets (e.g. through mobile advertising) (Marsden & Brown, 2023), and impeding efforts to ensure greater transparency, which is crucial to the regulation of digital business models and data markets (Feal et al., 2020).

Focusing on the data infrastructures that support mundane uses of mobile apps, the article builds on and contributes to the overlapping fields of critical data and app studies (Dalton & Thatcher, 2014; Dieter et al., 2019; Kitchin & Lauriault, 2014). We promote a timely infrastructural turn in critical data studies, (Flensburg & Lomborg, 2023) showcasing and discussing how power in mobile infrastructures can be located at the technical level. Our analysis specifically addresses the methodological opportunities and obstacles to ongoing monitoring of backend digital tracking. These methodological issues extend and add further complexity to ongoing debates over access to platform APIs, (Bruns, 2019) and especially to the differences in the data practices of iOS and Android operating systems and apps (Kollnig et al., 2022a). The article thereby also provides a much-needed methodological and epistemic perspective on recent efforts to tighten the regulation of the global data economy.

The article is structured as follows: first, we lay out the theoretical and methodological conditions for studying third-party services as a critical, but often overlooked, component of the mobile infrastructure and market. Second, and building on empirical examples from the Datafied Living project, we compare the conditions for accessing, collecting, and analysing SDKs in iOS and Android apps, asking what types of information can be accessed through the current state of the art in static SDK analysis, what information is (not) available, and how this may be explained with reference to the infrastructural arrangement and the constant tweaks and updates of the mobile operating systems. Our analysis lays bare the precarity of the methods for assessing SDKs as instruments of infrastructural power in digital tracking. We end the paper with a discussion of how the current conditions for accessing, collecting, and analysing reliable data on mobile infrastructures for

datafication influence our ability to challenge contemporary power structures and to develop effective tools for regulation and enforcement.

## Infrastructural power and (mobile) datafication

We approach mobile infrastructures for datafication through the theoretical concept of infrastructural power developed by Mann (1984) and others from the fields of sociology, development studies of, especially, state-sponsored infrastructures, science and technology studies (STS), and communication studies. In our work, we use it to put a spotlight on how operations at the backend material infrastructure of digital communication systems imply the exercise of power (e.g. Lomborg et al., 2023; Flensburg & Lai, 2023). Starting from a root level of technical, material infrastructure (Mansell & Plantin, 2022), we use the concept of infrastructure to identify the study of the architectural features of digital communication systems. We study the software development kits (SDKs) used in the mobile ecosystem, rather than specific platforms (e.g. iOS, Android). While we recognise that some platforms are becoming ‘infrastructuralised’ and almost indispensable (Plantin et al., 2018), we address infrastructure from the perspective of the political economy of communication – asking *who* controls key assets in the mobile app economy, here in the form of SDKs, and thus who acquires infrastructural power.

An actor holds infrastructural power to the extent that they have discretion over the design and functioning of an existing infrastructure (Law, 1990). Beyond the digital realm, this can be seen by looking at who is building and controlling traffic networks and, thereby, who decides the centrality and accessibility of different geographic locations and enables (or constrains) people’s abilities to get from a to b. In the case of mobile ecosystems, companies such as Alphabet and Apple exert control over its material underpinnings through designing and controlling system architecture, including setting the conditions for the integration of SDKs into apps. As will be evident in the analysis below, these companies exercise power in a number of ways through their technological operations. This effectively ensures their commercial consolidation as critical market actors and makes researching and regulating mobile infrastructures extremely challenging.

We see infrastructural power as intersecting with and complementary to platform power, and we draw upon this concept to highlight the fact that the power of big tech is to a great extent a matter of its dominance in offering critical infrastructure at the core of societal communication. This infrastructural power in turn contributes to consolidating its sizeable user bases and market dominance. Infrastructural power is structurally embedded and enables big tech to shape society from

within: we are currently witnessing a strong push in the public sector in European welfare societies, for instance, for optimisation and efficiency through digitalisation. This quest for optimisation can be seen as largely mirroring the ideology of the tech industry: tech solutionism and the idea that everything can be optimised with technology (e.g. Powell, 2021).

## SDKs as instruments of infrastructural power

While the power of operating systems or app store operators has been addressed by both research (Poell et al., 2019) and regulation (European Commission, 2018), the underlying data infrastructures, including SDKs, have attracted less attention. SDKs are bundles of programming code, code samples, documentation, and so forth, that allow developers of applications to implement functions from a third party into their applications (IBM Cloud Education, 2021). For many SDKs, a large part of the codebase exists outside of the app, akin to APIs, and outside the “view” of the developers. Like the more well-known web cookies, SDKs are key material components of mobile infrastructures that enable app functionality, security, and access to data collection and distribution (Pybus & Côté, 2022; van Kleek et al., 2017). This allows for faster app development as developers do not have to build things “from scratch”, and it allows an app to function with specific hardware and to provide the services that are widely used in the mobile app infrastructure (IBM Cloud Education, 2021). This, in turn, makes SDKs a critical asset for mobile tracking, and by extension for the acquisition of infrastructural power (Dieter et al., 2021; Flensburg & Lai, 2023). They also provide a useful entry point for exploring the dependencies between small actors and big tech providers in the app economy (Aradau et al., 2019).

SDKs have a variety of functions in an app. Pybus & Côté (2024) offer a taxonomy of SDKs: *programmatic adtech SDKs* that enable monetisation through tracking, e.g. the Batch SDK, an engagement platform with live user tracking and personal experience services (Batch, n.d.), Branch SDK, a deep linking platform with user tracking (Branch, n.d.), and Unity Ads, a platform for implementing apps and monetisation into apps/mobile games developed with the Unity engine (Unity, n.d.); *SDKs for app development*, including SDKs that enable the integration of APIs, cloud access, database support, and machine learning such as ChatGPT or Google Firebase; and *app extension SDKs* that enable authentication, social media plugins, payment and so forth. In addition, Pybus & Côté (2024) enlist so-called *super SDKs* which are multipurpose and integrate a suite of services. A prominent example is the Google Firebase Analytics SDK which allows the app developer to collect detailed user-specific data including: user actions, segmentation, revenue tracking, and most im-



portant, the integration of Google Analytic metrics into other Alphabet services like Google Mobile Ads (Google Developers, n.d.a, n.d.b). Another frequently used SDK is the Facebook SDK for Android/iOS allowing integration with Facebook's user authentication service, share functions, engagement, and Facebook-specific advertising (Meta, n.d.). To this we would add a fifth category of SDKs, *functional* SDKs, which comprises SDKs that are abundant in mobile applications as they are crucial for developing applications in the current mobile app system. An example of an SDK from this category is the general-purpose iOS SDK, provided by Apple through the Xcode Integrated development environment (IDE), a software program that assists the development of iOS applications. The iOS SDK is needed for an application to interact with the hardware and software system on Apple iPhones and is therefore paramount for the development of iOS applications. On Android systems the counterpart is called the Android SDK and is provided through the Android Studio IDE. Some error or crash handling SDKs are also found in this category.

## **Studying SDKs as core elements in mobile infrastructures for datafication**

When seeking to understand infrastructural power in contemporary digital societies, the gradual shift from web to app-based communication — and tracking — constitutes an important challenge for research and regulation alike. While digital methods for studying websites are relatively well established (Rogers, 2013), research designs for analysing the infrastructural architectures underpinning mobile apps are still under development (Dieter et al., 2019). Because apps reside in more closed-off ecosystems than websites, empirical interventions into mobile infrastructures and business models are restricted by the commercial interests of those who control, for instance, the types of information available in the app store and its APIs or the information visible in the app's code. Due to the proprietary nature of different app ecosystems (most prominently Apple's and Alphabet's), and the restrictions enforced by app stores and operating systems, there are no general, stable methods for mapping and measuring mobile tracking across operating systems.

As the go-to object of analysis for analysing mobile tracking, the Android operating system is designed as an 'open source' architecture that allows for unpacking individual apps and studying their code, including the presence of various types of third parties (Binns et al., 2018). As a result, publicly available databases are built on the basis of the Google Play app store, making access to insight into the data infrastructures and markets of Android apps comparatively easy. As we will elabo-



rate below, existing databases and libraries containing information on third-party services in Android apps are far from perfect and have significant limitations, especially when using them outside well-researched contexts such as the US. However, they do provide a methodological foundation for further improving and enriching empirical efforts at monitoring the mobile data economy.

Although recent efforts have been made to produce similar data on iOS apps (Kollnig et al., 2022a), Apple's infrastructure constitutes a more closed-off environment as a result of the historical legacies and strategies of the company. In recent years, Apple has introduced various measures to enhance user privacy and transparency, including providing information on the use of different types of data and features enabling users to opt out of third-party tracking (Kollnig et al., 2022b). However, as our examples below show, external third-party services continue to be an integral part of the iOS ecosystem.

While the two operating systems and their associated app stores now provide similar user and developer experiences, the open source traditions of Android and Apple's walled garden strategies continue to influence the conditions for studying their infrastructural foundations for communication. In effect, researchers, regulators, and other stakeholders interested in understanding contemporary mobile tracking ecologies need to develop and apply different methodological frameworks to fit the different empirical realities of the two systems; this is especially important if we are to understand the infrastructural implications of running either one of them on a personal device.

Current efforts to empirically investigate mobile infrastructures for datafication is highly interdisciplinary and comprises contributions from computer science, as well as social sciences and humanities research. Empirical studies use two distinct methodological approaches: dynamic and static analyses (Dieter et al., 2019; Gerlitz et al., 2019). The dynamic approach seeks to make sense of the systems, technologies, and business models of particular apps by sniffing data traffic to and from individual devices and domains (see e.g. van Kleek et al., 2017; Weltevrede & Jansen, 2019). Providing detailed information on specific in- and outbound flows and exchanges of data, these kinds of studies aid researchers in understanding what the mobile data infrastructure is made up of and how it operates.

The dynamic analysis approach can be used to find evidence of undiscovered SDKs as the data output is significantly smaller than from the static analysis. Conversely, it is less suited for studying the broader ecosystems of mobile apps and third-party tracking that go beyond individual apps and particular dataflows (Binns, 2022). In

developing valid methods for monitoring – and ultimately regulating – mobile infrastructures for datafication, the static approach constitutes a more suitable entry point.

In contrast to the dynamic approach, static analyses do not identify specific in- and out-bound data flows, but instead examine the software of apps to identify how data *can be* collected and distributed through the required user permissions and SDKs integrated into the app (Binns et al., 2018). This allows researchers to, for instance, compare tracker infrastructures and markets across web and app environments (Binns et al., 2018) or to draw up the contours of the market for mobile third-party services by studying the SDKs of global top app lists (Blanke & Pybus, 2020; Flensburg & Lai, 2022). For example, previous research in the field of computer science, particularly cyber security research, has explored mobile apps using static analysis methods and predominantly focuses on developing tools for identifying malicious code, detecting bugs (faulty code), and developing diagnostic techniques for analysing large quantities of apps and their associated metadata (Chen et al., 2016; Egele et al., 2011; Han et al., 2013).

In our analysis, we will draw on both techniques. However, as we will elaborate below, analyses of market power and competition structures in mobile tracking markets come with a variety of methodological challenges and epistemic problems – not least, when it comes to studying iOS apps and comparing them to those developed for the Android system.

## **The study: Infrastructural power in mobile apps in the Danish welfare state**

In exploring the infrastructural power exerted in and through SDKs and the methodological obstacles such research interventions entail, we build on an ERC-funded research project, Datafied Living. The project charts mobile infrastructures for datafication in the welfare state of Denmark and connects infrastructural developments to people's experiences of tracking and datafication across personal, work, and institutional domains. Having followed 69 main research participants in the field for a year, one part of the project maps their use of mobile apps as a means for investigating the underlying data infrastructures and third-party markets that are often considered invisible and opaque. The research participants kindly allowed us to inspect all apps installed on their phones and build a database from them. The database consists of 1,129 apps across the Android and iOS phones owned by our participants. As an extension to this work, we also collaborated with the Danish Data Ethics Council on applying the knowledge gained from

the project to scope the prospects for increasing the monitoring of the mobile app and data market.

Denmark is one of the most digitised nations in the world. As a prime example of a so-called universalist welfare state (Esping-Andersen, 1990), the state has historically played a proactive role in advancing principles of equality, citizen autonomy, and decommodification through regulation. At the same time, research suggests that the ongoing datafication of society threatens such principles and is in the process of reconfiguring the welfare state (Dencik, 2022), as a wide range of key welfare services increasingly rely on services and infrastructures that are governed on the basis of commercial values and logics (Otto, 2023). This is certainly the case in Denmark, where there has been a strong push to transition to digital government with “digital ready” legislation and a willingness to partner with international commercial actors to facilitate this transition; developing systems of digital governance, however, have not kept pace. Considering the possibility for monitoring infrastructures for datafication in the interest of citizens, Denmark arguably constitutes a critical case for studying the tensions between state regulation and commercial interests in the digital age.

To illustrate the empirical potential and pitfalls from the methods explained in this paper and to exemplify the integration of third-party SDKs, we use a subset of our main sample consisting of five apps connected to the Danish welfare state: “Aula”, “Min Sundhed”, “e-boks”, “mit.dk”, and “mitID”, which were all commissioned by the Danish state through different government contractors. These five apps were chosen as they represent prime examples of the digital welfare state in which citizens rely on digital applications like these to communicate with welfare state institutions across different domains of everyday life. Based on these examples, the remainder of the article offers methodological insights into the analysis of third-party SDKs across iOS and Android, focusing on the opportunities and challenges regarding data access, collection, and analysis with implications for data quality in studies of SDKs. As such, we contribute to the ongoing work to create methodological roadmaps for identifying third-party services in Android and iOS apps (Kollnig et al., 2022a) as a basis for the systematic monitoring of infrastructural power.

## Methodological pathways for SDK analysis

In identifying and analysing SDKs within and across mobile apps, we encountered multiple methodological obstacles that influence the data quality and the validity of the empirical findings. These methodological challenges can roughly be divided

into three categories, reflecting the classic steps in any empirical study, namely: 1) how data can (and cannot) be *accessed* including assessing the available tools and services used to gain insights into the software code of particular apps; 2) how data can (and cannot) be *collected* and *sampled* including questions about how to construct reliable libraries and databases to look up identified SDKs; and 3) how data can be *analysed* and *interpreted* including reflections about the knowledge that these methods can (and cannot) generate. Throughout the analyses, the differences between the Android and iOS systems will be highlighted as each ecosystem constitutes different gateways for accessing, collecting, and analysing apps; similarly, their different business models affect what opportunities there are for empirical interventions. In discussing the methodological obstacles, we will generally focus on the static analysis method.

### **Data access: setting up the technical framework for SDK analysis across iOS and Android**

As mentioned above, there are significant differences in the types of data that can be accessed through the iOS and Android operating systems, and by extension in the knowledge that can be gained about apps published in the different app stores and running on different devices. In fact, we see the gatekeeping of the access to data as a key example of infrastructural power, since the technical setup for data access serves as a precondition for developing and publishing tools, databases, and resources available to the public and to researchers. The lack of publicly available data on iOS apps – compared to that of Android apps – is directly connected to the ways Apple governs and controls access to information about the software installed in individual apps. We see the data access process as the technical setup for accessing the analytical object, which is the software of the mobile application.

As is evident from several previous studies, ventures into studying mobile infrastructure through SDKs often start with Android (Binns et al., 2018; Pybus & Coté, 2022; Weltevrede & Jansen, 2019). The openness of the Android OS has enabled the development of, for instance, the non-profit privacy auditing platform, Exodus Privacy<sup>1</sup>. As a publicly available website that allows users to look up individual Android apps and disclose identified SDKs, Exodus substantially shortens the path from data access to analytical results.

By comparison, analysing iOS applications and their installed SDKs is much more complicated (Kollnig et al., 2022a). To download iOS apps from the AppStore to

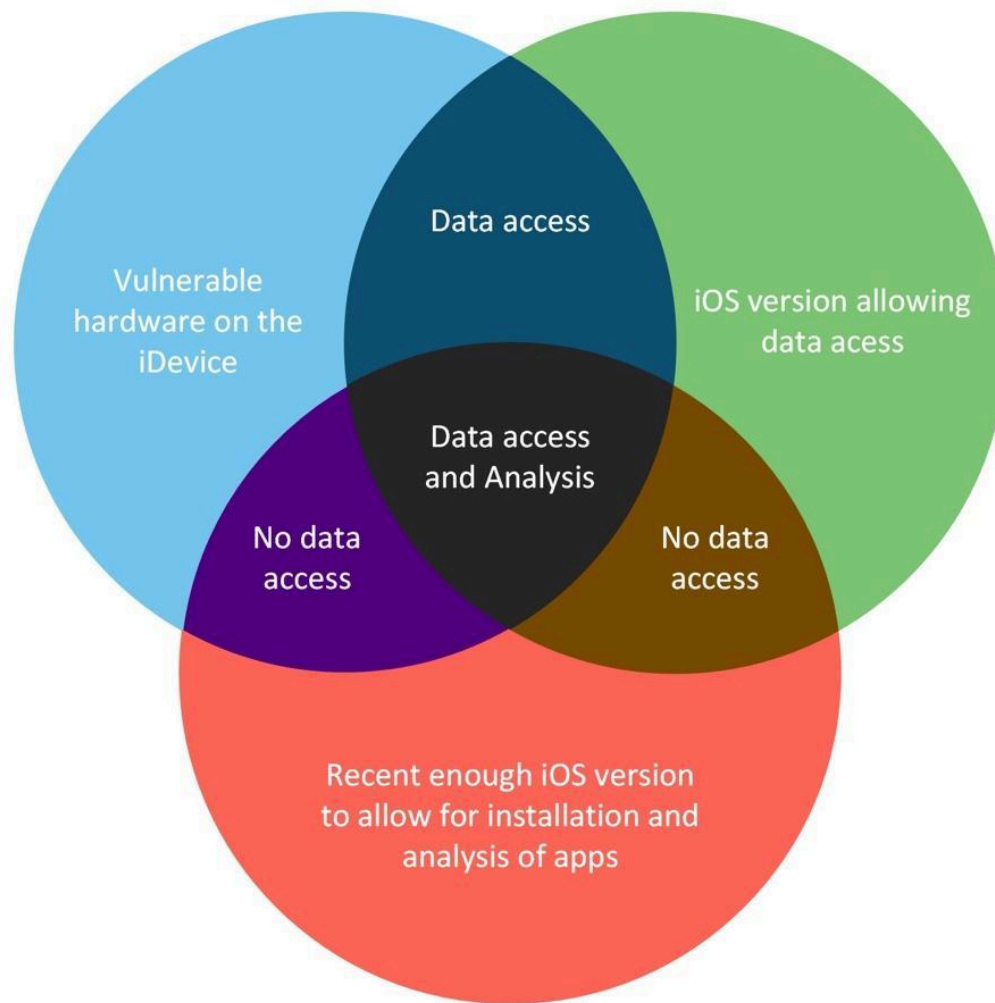
1. For more information see Exodus Privacy (n.d.a.).

the computer, an AppleID with a verified email and phone number is required, as is a mobile device running iOS, a MacOS computer with Xcode<sup>2</sup>, and Apple's IDE for iOS. The program `ideviceinstaller` by `libimobiledevice`<sup>3</sup>, a free and open source library designed to communicate with iOS devices, can then be used to install the applications on the iOS device. For this to work, however, one has to unlock the security systems that Apple implements in iOS, a procedure which is generally used to install apps from outside the Apple App Store or to access functionality that is not accessible through the iOS user interface.

When experimenting with identifying SDKs in the app sample from the Datafied Living project (where the majority of the participants, like the Danish population in general, are Apple users), unlocking Apple's security system is a prerequisite. Furthermore, an unlocking procedure, for instance the program `Frida-server`, is needed to install some of the communication software on the phone. The `Frida-server` allows you to communicate with the iPhone in the data extraction process (Ravnås, 2023). More specifically, `Frida` consists of a set of tools that can inject code into programs that are running without decompiling the source code. As the `Frida-server` is not available on the Apple App Store, the phone needs to be compatible with a working third-party store/repository manager. As a consequence of the lack of stable and modern releases of working repository managers for newer iPhones, reproducing the method may be challenging. Through the design iterations of both iPhone hardware and iOS software, Apple has patched the vulnerabilities that otherwise made these kinds of interventions possible. This means that only a limited range of older iPhones running past iOS versions *can* be used for data collection. In short, the iPhone used for analysis will essentially have to be in a sweet spot or "goldilocks" zone, visualised in the Venn-diagram below (Figure 1).

2. For more information see Apple developer IDE Xcode (n.d.).

3. `Libimobiledevice` is a cross-platform FOSS library for interacting with iOS devices. In this project "`ideviceinstaller`" is used. For more information see `Libimobiledevice` (n.d.).



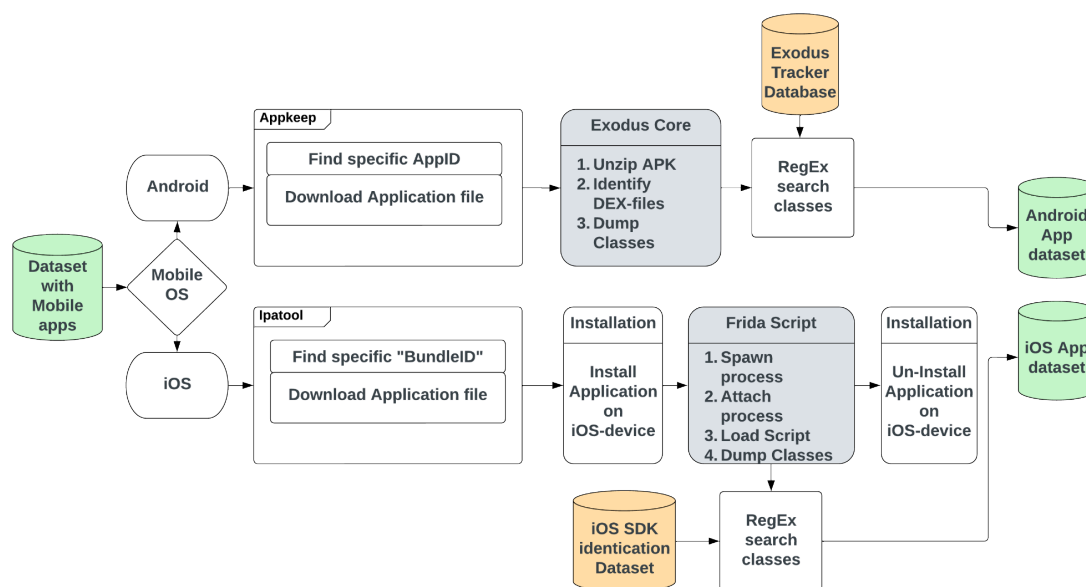
**FIGURE 1:** Enabling and constraining factors for accessing information on SDKs.

Lastly, depending on the size of the initial sample and the research question, automation of the data collection might be required. With a large sample of apps, which would be relevant for public monitoring and regulatory purposes, automation of the analysis will almost certainly be necessary as manually analysing apps by installing and extracting data would be exceptionally time consuming. However, automating the process of analysing iOS can prove challenging because of, for instance, permission prompts where the user needs to accept or decline permissions to give, for example, GPS location, or unexpected crashes caused by unlocking Apple's security system. In sum, there are a number of technical obstacles to accessing the app code from which SDKs can be extracted for analysis, in particular in relation to the iOS operating system.

### **Sampling and data collection: how to identify an SDK**

Regardless of whether the data is accessed through Exodus Privacy (for Android

apps) or by means of an older version of the iPhone (for iOS), the data collection follows three steps: 1) preparing the app sample by contextualising app names; 2) installing and extracting data from the app; and 3) identifying known SDKs in the extracted data. Figure 2 illustrates the specific procedures involved in each of these steps for Android and iOS apps.



**FIGURE 2:** Data collection procedures for locating SDKs in Android and iOS apps.

Focusing on the first step of the data collection process (the left-hand side of the figure), the sampling strategy for identifying SDKs in apps depends on the nature and purpose of the research. If you are interested in the most widespread SDKs, for instance, you might simply sample apps from the lists of top downloads in the Apple App Store and Google Play store that typically contain individual appIDs referring back to the app store in question<sup>4</sup>. When working with a list of apps derived from people's phones, as in our case, these apps need to be matched with the right app in the app stores. While an app on the Google Play store or the Apple App Store must be unique, app names like "Calculator – Free" and "Calculator – Plus" are not uncommon. This means that several results will be obtained when searching for the given app name and the chance of getting false positives is high. Here, the ID of the app can ensure that the identified app is also the correct one.

To identify exact appIDs, we suggest two methods, one each for iOS and Android apps. For iOS, a tool called "ipatool"<sup>5</sup> is used. Ipatool is a command line tool (CLI)

4. See e.g., Androidrank.org (n.d.).



that functions as a wrapper for the iTunes API, allowing for the lookup of app information, and functions as an emulation of a macOS AppStore so enabling the user to download app packages. The tool can use the name of an app and return the search results from the app store. For Android, the appID can be read in the Google Play store URL for each app; however, for a more automated approach the “gpapi” tool can be used<sup>6</sup>. The output of the searches will then have to be manually examined to ensure that the correct ID is attributed to the targeted app in the sample. To summarise, Table 1 lists the five apps sampled for this paper, including their respective iOS and Android IDs.

**TABLE 1:** Public sector app sample with corresponding appID for iOS and Android

APP	IOS ID	ANDROID ID
mit.dk	com.netcompany.mit.view-client	com.netcompany.mitdk
MinSundhed	dk.sundhed.minsundhed	dk.sundhed.minsundhed
MitID	dk.mitid.app.ios	dk.mitid.app.android
Aula	com.netcompany.aula-native	com.netcompany.aulanativeprivate
e-Boks.dk	dk.eboks.eboks	com.eboks.activities

Once the required sample of app data is scraped, the presence of SDKs in the sample can be identified in the app code. This is done by extracting the signatures in the program code that correspond to *known identifiers* and *signatures of known* SDKs. At this point, again, there are significant differences between analysing either Android or iOS apps. As mentioned above, the Android static analysis relies heavily on the Exodus Privacy framework and uses the Exodus Core library and its tracker definitions to identify SDKs in the application (Exodus Privacy, 2018). This is accomplished by looking at the signatures in the application, which will be compared to known identifiers of SDKs. This is possible because the Android project and Google provides a program called “Dexdump,”<sup>7</sup> which can read the signatures in the program files without decompiling and installing the apps. The strength of the Android process is its stability as everything is executed locally on a computer with a Linux OS, with no need to connect to a phone.

The iOS static analysis is, again, substantially more complicated. The difficulty of

5. For more information on the CLI tool for identifying and downloading iOS apps, see IPATool (n.d.).

6. Google play python API (Gpapi), is a python package to search the Google Play store. For more information see Google play python API (n.d.).

7. Dexdump software, provided by Google / The Android Open Source Project. For more information see Dexdump (n.d.).

analysing iOS applications compared to Android is partly due to there being no easily available tool comparable to Exodus, and partly due to iOS not being built around an open source development paradigm. For iOS there is no “Dexdump” comparable program, as all apps are encrypted, so to extract the signatures in the app, the app must first be installed on the phone, and then by injecting a script into the application, the desired data can be extracted. When working with our sample of Danish welfare state apps, this allows us to open an application on an iOS device and to extract the signatures of all the internal functions of the specific application.

The last step in the data collection process is to identify the SDKs in the extracted data. In most modern programming languages, the naming of objects and variables is ordered in so-called namespaces. Within a namespace, definitions of, for instance, functions must be unique, which incidentally helps in the detection of SDKs through signatures as the signatures/object names must be unique across the program. To give an example, the identifier for the Google Analytics SDK will differ from the Facebook SDK in the extracted data but will be the same across applications that have the SDK incorporated. This is because the SDK is by design general purpose and must be easily documented and readable. For both the iOS and Android analysis, the extracted data for each app, which contains between 40,000 and 70,000 unique signatures, i.e. lines of text, are searched to find known identifiers of an SDK.

The Android analysis relies on the tracker (SDK) definitions provided by the Exodus database, while the iOS tracker definitions use a modified database made up of the PlatformControl Analyser iOS signatures (Kollnig et al., 2022a). The analysis requires knowing the specific code signatures of the SDKs to find them in the extracted data. As the results produced for each app consist of 40,000 – 70,000 unique signatures, it would not be feasible to manually search the extracted data for SDKs; therefore reporting SDK signatures relies very much on having already identified SDKs in a database comparable to Exodus’s against which the results can be compared. This restriction affects the results of the analysis as we are only able to identify SDKs that are known and widely used by developers.

This three-step process reveals a significant challenge for SDK research, namely how to generate a coherent and exhaustive dataset of SDKs from the sampled apps. The datasets generated using these methods are dependent on the quality of the underlying libraries, which are constructed by means of dynamic analyses (network sniffing) of data packages transported to different third-party domains. As such, many rare, emergent, or highly context-specific third-party services are most

likely to be invisible to static analyses like the ones discussed here. We cannot simply assume that existing libraries of SDKs for either Android or iOS are exhaustive. There are 428 identified SDKs in the current Exodus database for Android (Exodus Privacy, n.d.b), compared to the 98 identified SDKs in the current state of the art database of iOS SDKs (Kollnig et al., 2022a). The presence of fewer SDKs in the iOS database cannot simply be explained with reference to iOS being a more hostile environment for third-party tracking, but must be viewed against the backdrop of data access as explained above, making it difficult to automatically identify SDKs for iOS. It is an empirical question as to whether there are in fact fewer SDKs in iOS apps.

However, it is possible – if cumbersome – to augment the existing database for iOS by first conducting dynamic analyses of iOS apps through network traffic analysis or by using App Privacy Report<sup>8</sup>, a feature implemented in iOS 15.2 which makes it possible for users to examine an installed app’s network activity. At the same time, we note that while there is a larger SDK library provided by Exodus as a starting point for SDK analysis on Android, it has the same principal limitation: we cannot assume that the library of existing SDKs is exhaustive and complete. Furthermore, when using SDK databases, the underlying reasons for how databases are constructed and what constitutes valuable data can be different from the motivation of researchers using these databases. Exodus’ library, for instance, has been designed with the purpose of addressing privacy questions, while our research concerns looking at the broader questions about the evolving data infrastructures and ownership structures in the mobile app market.

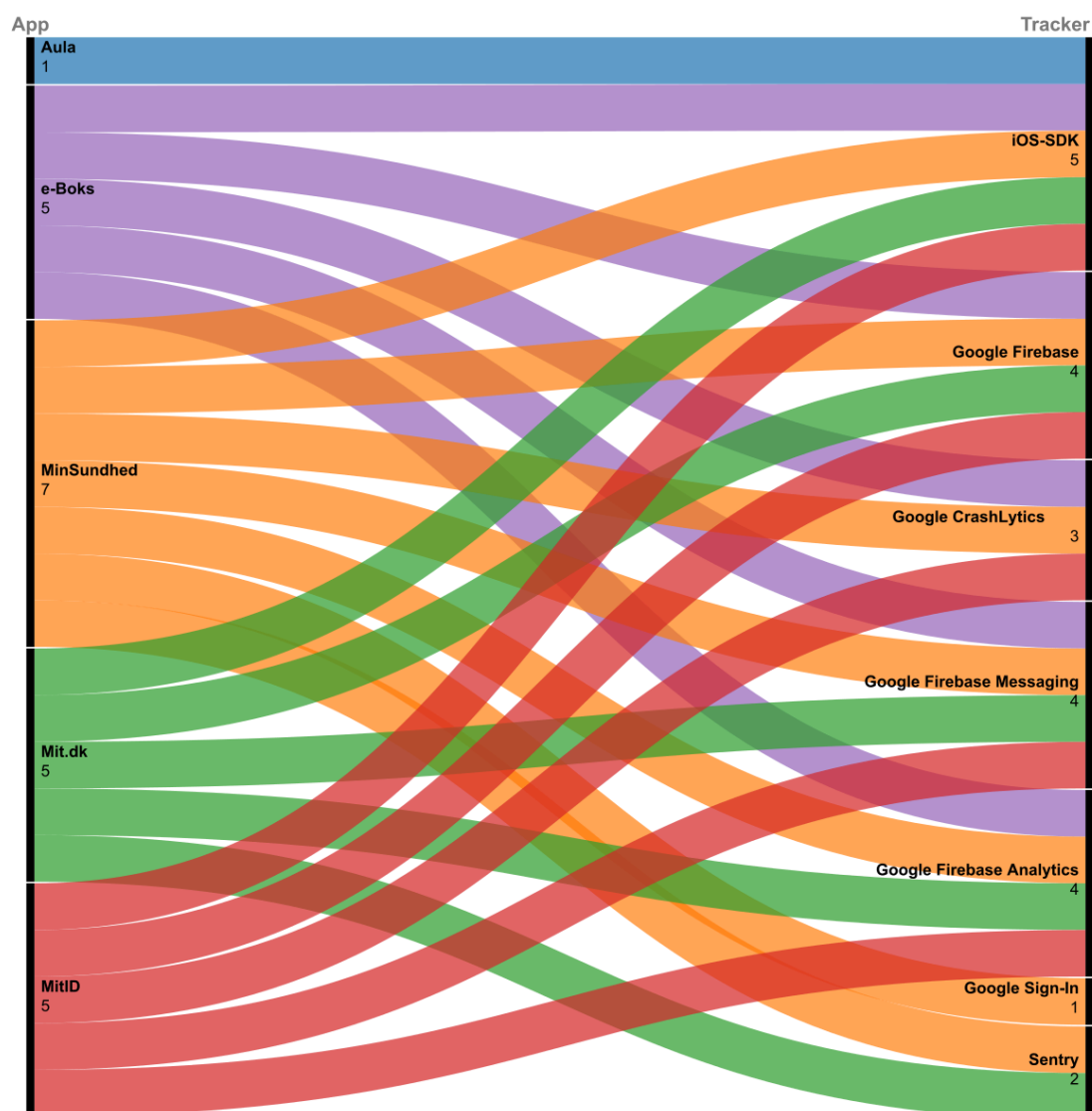
## **Data analysis: SDKs in Danish welfare apps**

Having constructed a dataset with SDKs identified in iOS and Android apps, the next, critical, step is to evaluate the information contained in them. Since databases have been constructed with the purpose of pushing mobile privacy discussions forward, SDK analyses will typically be able to present the relationship between a given number of apps, their embedded and identified SDKs, and the data industry actors who provide the SDKs and thus may be expected to be harvesting data from the app. This information can be used to map ownership and market structures in mobile infrastructures for datafication, as these look at a given time in a given context (and with the methods and libraries available to research).

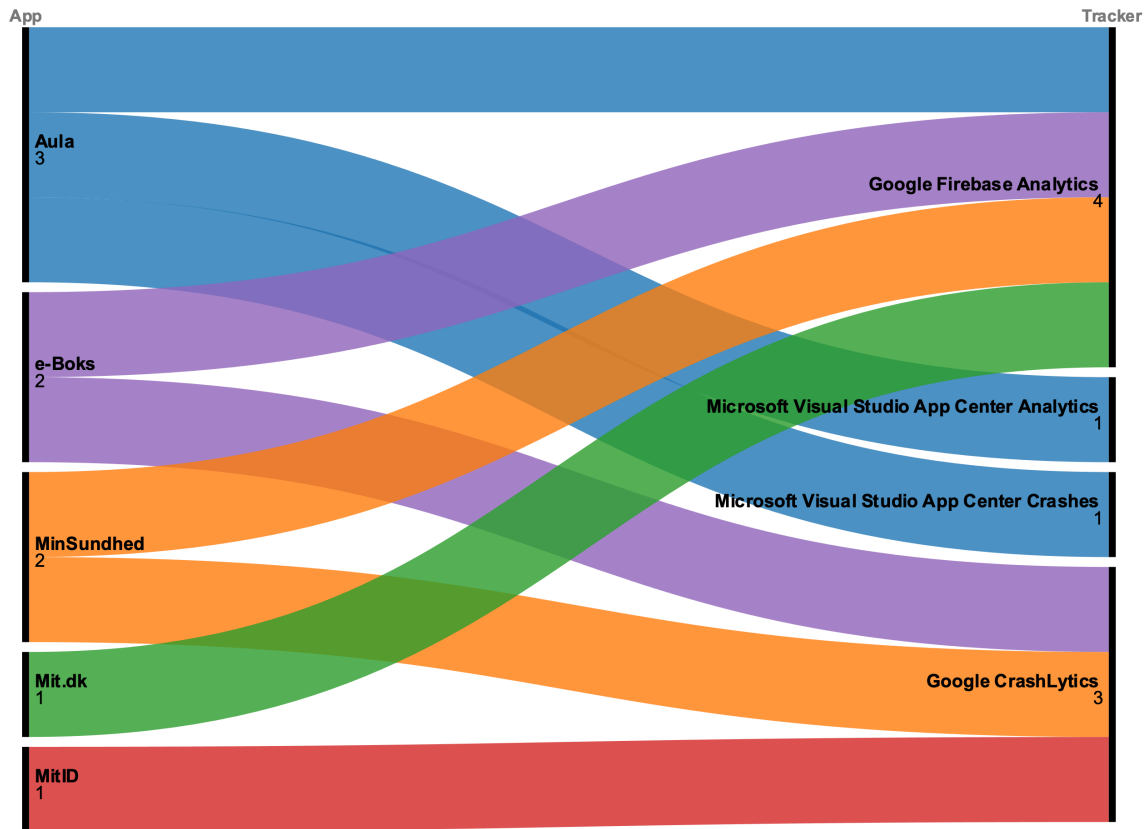
In our case, we are interested in expanding this type of analysis to map infrastruc-

8. For more information, see Apple Inc. (n.d.).

tural power in the digital Danish welfare state: how commercial actors via SDKs are positioned to deliver key infrastructures for communication between citizens and public sector welfare providers. Using an illustrative subsample of apps that are crucial for citizen access to public welfare in Denmark, we can show how state institutions have come to rely on commercial market actors when digitising key welfare services. Figures 3 and 4 below illustrate how what is often assumed to be public infrastructure for healthcare, education, government communication, personal authentication, and so forth does not go unaffected by third-party actors. In fact, each app (left side of the figures) embeds externally supplied SDKs (right side of the figures), most of them provided by Alphabet and Microsoft.



**FIGURE 3:** iOS versions of Danish welfare state apps and their SDKs identified through static analysis.



**FIGURE 4:** Android versions of Danish welfare state apps and their SDKs identified through static analysis.

As is evident from Figures 3 and 4, the Google Firebase Analytics SDK and its subsets dominate while Google Crashlytics is close behind. But there are other actors as well. On iOS, two of the apps, “mit.dk” (an app for reading electronic mail from the Danish government) and “Min Sundhed” (an app for communicating with the Danish healthcare system), use the privately developed Sentry, an SDK for error tracking and assessing code and operation performance<sup>9</sup>. Both figures show that, at the level of mobile apps interfacing between citizens and core welfare services (health, education, etc.), the Danish welfare society has become critically dependent on commercial providers of a key material component of the infrastructure: SDKs that allow developers to implement and use the same functionality and services used by the wider mobile application market. As noted earlier, utilising SDKs as a development practice, and especially utilising SDKs from large Platform companies like Google, is not the sole option but the pragmatic and low cost choice for developers when implementing the desired functions.

While this raises the obvious questions about data protection and privacy, our

9. For more information, see Sentry Documentation (n.d.).

analysis of the technical operations of SDKs suggests that we need to move beyond such issues and address the infrastructural grab that puts Big Tech at the core of digital systems for welfare. This grab is similar to that which has previously been documented in the context of smaller and medium-size businesses becoming desperately dependent on Big Tech for supplying their mobile services (Blanke & Pybus, 2020; Lai & Flensburg, 2021). In effect, this means that when welfare institutions and nationally-commissioned developer studios use ready-made services for developing apps, processing data, and keeping services running smoothly, they transfer infrastructural power to corporate enterprises that are subject to very little democratic control. As evident from a number of examples in Denmark (Datatilsynet, 2024; Olifent, 2023), public authorities experience significant problems with ensuring that personal data is used legally, and they have very little room for manoeuvre when prices on services from American Big Tech corporations continue to rise. In addition, the presence of third parties in welfare apps invites further critical analysis, not only to find out how specific data types are allowed to flow through them but also how apps are developed and how code is reused across digital ecosystems in general (Aradau et al., 2019).

As illustrated in the figures above, our microscopic case study – somewhat surprisingly – finds a higher prevalence of SDKs in the iOS versions compared to the Android versions of the same apps. For instance, we only identify the Google Firebase Analytics SDK in the Android version of the identification app MitID, but find seven different SDKs in the iOS version. One explanation for this difference might be the extent of the different databases and their respective definitions of a ‘tracker’. Another possible explanation is that the SDKs might perform different operations across the two operating systems; for example, SDKs owned by Alphabet may be more multipurpose on Android apps than on iOS apps, reflecting the rise in so-called “super SDKs” as suggested by Pybus & Côté (2024). Finally, there might be differences in the versions of the apps analysed. For example, the Android version could be older than the iOS version, as Android apps tend not to be redeveloped at the same pace as iOS apps. The relatively few SDKs in the iOS analysis of the Aula app might also indicate a gap in the libraries as the Android version has both Google Firebase Analytics and Microsoft SDKs embedded.

To check the findings and mitigate the challenges of using existing libraries to identify SDKs, we also performed a dynamic analysis on the iOS versions of the five Danish welfare apps by intercepting the network calls made by the app and analysing the domain of the calls. However, the dynamic analysis had a specific methodological limitation, in that these apps are heavily protected against the un-

derlying processes employed by the method, namely the intercepting proxy used to route network traffic through certificates, meaning that the apps would crash if they detected that a certificate was invalid. However, the dynamic analysis supports the findings from the static analysis in that all of the identified SDKs also appear in the static analysis except for the SDK “nStack”, which does not exist in our SDK library. This, in turn, explains why “nStack” was not identified in the static analysis, and testifies to the limits of the static approach – and highlights the dependency of static analysis on regular dynamic interventions. Without conducting dynamic analyses to identify new or altered SDKs, the validity of the libraries used for the static identification of SDKs will be weak.

The limitations and uncertainties described in the results all point back to the methodological challenges listed above. Due to the lack of comprehensive SDK databases and libraries, we cannot make definite comparisons between Android and iOS apps, meaning that the figures above are only empirical indications of a reality that might be much more complex. A related challenge is that third-party service providers are notorious for changing the names of their products. In other words, more work is needed if we are to develop methods that can ground actual, systematic market monitoring and qualify regulatory intervention. To that end, a crucial next step is to expand the SDK libraries and develop ways of detecting new SDKs, for instance by using the information made available in the privacy settings menu on Apple devices or by doing extensive dynamic analyses.

Despite the obvious and manifold challenges of doing SDK analyses, our empirical experiments can make a valuable contribution to the ongoing political discussions about the future of digital and datafied societies. Returning to the public accountability issues at the “root” level of the communication infrastructure (Mansell & Plantin, 2022), we can put the spotlight on the widespread use of externally supplied SDKs, even in core welfare state sectors. This not only means that state institutions are becoming increasingly dependent on a small number of US-based and commercially run tech companies but also increases the market advantages and dominance of these companies while simultaneously legitimising their data practices (Blanke & Pybus, 2020). By collaborating with Danish authorities, such as the Data Ethics Council, we can use the empirical examples and methodological pathways (and dead ends) to show ways forward to increase monitoring, and ultimately, wrest back democratic control from this largely opaque and unregulated market.



## Conclusions and perspectives: monitoring data infrastructures with precarious methods?

This article has discussed the prospects and pitfalls of empirically analysing third-party tracking in mobile apps through detecting SDKs as key entry points for studying infrastructural power. Understanding how third-party tracking operates in mobile ecosystems and how data flows are enabled and constrained across apps and operating systems is critical for any political or regulatory intervention aimed at benefiting human flourishing in today's digital society. In our pursuit to understand and govern the increasingly concentrated market structures in the mobile ecosystem (Flensburg & Lai, 2022), systematic and reliable monitoring is pivotal for providing a knowledge base to guide regulatory initiatives and ensure the legitimacy of such regulation. To acquire this knowledge, we need to understand the technological characteristics of, in this case, SDKs and define their role in the greater digital ecosystem and economy.

Laying out methodological and empirical pathways for future SDK analyses, we have identified multiple bumps on the road ahead. These include the fundamental differences in data access, with implications for comparing SDKs across operating systems and app stores, problems relating to constructing reliable datasets, and limitations in the knowledge they can generate. As a general conclusion, the current methodological conditions for studying SDKs mean that we have no guarantee that the data we collect is comprehensive and reflects actual market structures in the mobile data economy. That is to say, empirical analyses using the methods outlined here can only provide indications of the SDK market and sensitise us to who the powerful actors might be, but do not cover the full range of actors and operations in the mobile data market. This constitutes a fundamental problem for regulators who seek to identify and sanction dominant market actors since any measurement of, for instance, the prevalence of a particular SDK provider is easy to contest.

Our discussions about data access, collection, and analysis suggest that the infrastructural operations of Apple and Alphabet amplify an already skewed power balance in the mobile app and data market. The providers of operating systems and app stores hold the power to set up the fundamental conditions that app developers (including welfare state institutions) are forced to accept. For instance, when restricting the use of third-party services (as Alphabet has done with cookies in the Chrome browser and Apple has done with App Store), they simultaneously close off markets where they themselves dominate and which are notoriously difficult (and sometimes legally tricky) to intercept. This is the essence of infrastructural

power. Our illustration of the presence of commercial actors in the public welfare sector in Denmark suggests that we urgently need to ask questions about the long-term implications of this power grab for the public values underpinning the welfare state.

In this sense, our study resonates with existing work on the power of platforms (van Dijck et al., 2018) and their deliberate strategies of obfuscation (Draper & Turow, 2019), while also drawing our attention to the role of technical-material infrastructure in the exercise of power. By controlling what information is available and how it is (not) accessible, Big Tech constructs the conditions that shape how they can be monitored and ultimately regulated. The infrastructural operations of dominant actors in the mobile ecosystem laid out in our analysis of SDKs not only impede transparency, systematic democratic monitoring, and possible regulation of an increasingly critical societal infrastructure; they also limit the critical capabilities of researchers and of open source and hacker environments, which are constantly forced to adjust their counterintelligence measures and tools to be able to inspect mobile infrastructures for datafication (Aradau et al., 2019).

Regulatory efforts targeting individual cases, as per the Google Analytics example at the beginning of this article, suggest there is prospect of increasing political momentum to reign in tracking. But to fuel such momentum and ensure regulatory efficiency we need to target the infrastructural root level. Systematic monitoring of third-party tracking in the mobile ecosystem, its purposes and market dynamics, is a necessary condition for developing adequate, evidence-based policy and regulatory interventions that protect citizens from unwanted data capture, and expose the infrastructural power of big tech. As a final note and possible future direction for research and policy, we suggest an alternative strategy than the one presented here. Building on the technical knowledge gained from reverse engineering experiments and studying the backends of mobile apps from the *outside*, future initiatives should aim at requiring app store and operating system managers to make the information available to researchers and regulators. Rather than having to rely on volatile and precarious methods for detecting third-party operations in apps, the recent momentum for political intervention could push the responsibility for ensuring the quality, reliability, and comparability of data on SDKs back onto the infrastructure providers. This requires a clear understanding of what exactly to ask for and how to interpret what can be returned. We hope that this article can contribute to achieving these aims.

## References

Androidrank. (n.d.). *List of Android most popular Google Play apps*. <https://www.androidrank.org/android-most-popular-google-play-apps>

Apple Developer. (n.d.). *Xcode 15*. <https://developer.apple.com/xcode/>

Apple Inc. (n.d.). *About App Privacy Report*. <https://support.apple.com/en-al/HT212958>

Aradau, C., Blanke, T., & Greenway, G. (2019). Acts of digital parasitism: Hacking, humanitarian apps and platformisation. *New Media & Society*, 21(11–12), 2548–2565. <https://doi.org/10.1177/1461444819852589>

Batch. (n.d.). *About us*. <https://batch.com/about>

Binns, R. (2022). Tracking on the web, mobile and the internet of things. *Foundations and Trends® in Web Science*, 8(1–2), 1–113. <https://doi.org/10.1561/18000000029>

Binns, R., Zhao, J., Kleek, M. V., & Shadbolt, N. (2018). Measuring third-party tracker power across web and mobile. *ACM Transactions on Internet Technology*, 18(4), 1–22. <https://doi.org/10.1145/3176246>

Blanke, T., & Pybus, J. (2020). The material conditions of platforms: Monopolization through decentralization. *Social Media + Society*, 6(4). <https://doi.org/10.1177/2056305120971632>

Branch. (n.d.). *What is Branch?* Branch Help. <https://help.branch.io/using-branch/docs/what-is-branch>

Bruns, A. (2019). After the ‘APIcalypse’: Social media platforms and their fight against critical scholarly research. *Information, Communication & Society*, 22(11), 1544–1566. <https://doi.org/10.1080/1369118X.2019.1637447>

Chen, K., Wang, X., Chen, Y., Wang, P., Lee, Y., Wang, X., Ma, B., Wang, A., Zhang, Y., & Zou, W. (2016). Following devil’s footprints: Cross-platform analysis of potentially harmful libraries on Android and iOS. *2016 IEEE Symposium on Security and Privacy (SP)*, 357–376. <https://doi.org/10.1109/SP.2016.29>

Dalton, C. M., Taylor, L., & Thatcher, J. (2016). Critical data studies: A dialog on data and space. *Big Data & Society*, 3(1). <https://doi.org/10.1177/2053951716648346>

Datatilsynet. (2022). *Afgørelse om brug af Google Analytics fra det østrigske datatilsyn* [Decision on the use of Google Analytics from the Austrian Data Protection Authority] [Press release]. <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/jan/afgoerelse-om-brug-af-google-analytic-s-fra-det-oestrigske-datatilsyn>

Datatilsynet. (2024). *Datatilsynet giver påbud i Chromebook-sag* [The Danish Data Protection Authority issues an injunction in the Chromebook case] [Press release]. <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2024/jan/datatilsynet-giver-paabud-i-chromebook-sag>

Dencik, L. (2022). The datafied welfare state: A perspective from the UK. In A. Hepp, J. Jarke, & L. Kramp (Eds.), *New perspectives in critical data studies: The ambivalences of data power* (pp. 145–165). Palgrave Macmillan. [https://doi.org/10.1007/978-3-030-96180-0\\_7](https://doi.org/10.1007/978-3-030-96180-0_7)

Dexdump. (n.d.). *DexDump.cpp*. Google Git. [https://android.googlesource.com/platform/dalvik.git/+a/android-4.3\\_r3/dexdump/DexDump.cpp](https://android.googlesource.com/platform/dalvik.git/+a/android-4.3_r3/dexdump/DexDump.cpp)

- Dieter, M., Gerlitz, C., Helmond, A., Tkacz, N., van der Vlist, F. N., & Weltevrede, E. (2019). Multi-situated app studies: Methods and propositions. *Social Media + Society*, 5(2). <https://doi.org/10.1177/2056305119846486>
- Dieter, M., Helmond, A., Tkacz, N., van der Vlist, F., & Weltevrede, E. (2021). Pandemic platform governance: Mapping the global ecosystem of COVID-19 response apps. *Internet Policy Review*, 10(3). <https://doi.org/10.14763/2021.3.1568>
- Draper, N. A., & Turow, J. (2019). The corporate cultivation of digital resignation. *New Media & Society*, 21(8), 1824–1839. <https://doi.org/10.1177/1461444819833331>
- Egele, M., Kruegel, C., Kirda, E., & Vigna, G. (2011). PiOS: Detecting privacy leaks in iOS applications. *Proceedings of the Network and Distributed System Security Symposium*. NDSS 2011, 18th Annual Network and Distributed System Security Symposium, San Diego, California. <https://www.ndss-symposium.org/ndss2011/pios-detecting-privacy-leaks-ios-applications-paper/>
- Esping-Andersen, G. (1990). *The three worlds of welfare capitalism*. Princeton University Press.
- European Commission. (2018). *Antitrust: Commission fines Google €4.34 billion for illegal practices regarding Android mobile devices to strengthen dominance of Google's search engine* [Press release]. [https://ec.europa.eu/commission/presscorner/detail/en/IP\\_18\\_4581](https://ec.europa.eu/commission/presscorner/detail/en/IP_18_4581)
- European Data Protection Board (EDPB). (2022). *The Danish DPA imposes a ban on the use of Google Workspace in Elsinore municipality* [Press release]. [https://www.edpb.europa.eu/news/national-news/2022/danish-dpa-imposes-ban-use-google-workspace-elsinore-municipality\\_en](https://www.edpb.europa.eu/news/national-news/2022/danish-dpa-imposes-ban-use-google-workspace-elsinore-municipality_en)
- Exodus Privacy. (2018, August 17). *Exodus static analysis*. [https://exodus-privacy.eu.org/en/post/exodus\\_static\\_analysis/](https://exodus-privacy.eu.org/en/post/exodus_static_analysis/)
- Exodus Privacy. (n.d.a). *Exodus Privacy: Analyzes privacy concerns in Android applications*. <https://exodus-privacy.eu.org/en/>
- Exodus Privacy. (n.d.b). *Trackers*. <https://reports.exodus-privacy.eu.org/en/trackers/>
- Feal, Á., Gamba, J., Vallina-Rodriguez, N., Wijesekera, P., Reardon, J., Egelman, S., & Tapiador, J. (2020). *Don't accept candies from strangers: An analysis of third-party SDKs*. Computers, Privacy and Data Protection Conference (CPDP 2020), Brussels, Belgium. <https://doi.org/20.500.12761/779>
- Flensburg, S., & Lai, S. S. (2023). Follow the data! A strategy for tracing infrastructural power. *Media and Communication*, 11(2), 319–329. <https://doi.org/10.17645/mac.v11i2.6464>
- Flensburg, S., & Lomborg, S. (2023). Datafication research: Mapping the field for a future agenda. *New Media & Society*, 25(6), 1451–1469. <https://doi.org/10.1177/14614448211046616>
- Gerlitz, C., Helmond, A., Nieborg, D. B., & van der Vlist, F. N. (2019). Apps and infrastructures – A research agenda. *Computational Culture*, 7. <http://computationalculture.net/apps-and-infrastructure-s-a-research-agenda/>
- Google play python API. (n.d.). *Googleplay-api* [Repository]. Github. <https://github.com/NoMore201/googleplay-api>
- Han, J., Yan, Q., Gao, D., Zhou, J., & Deng, R. H. (2013). Comparing mobile privacy protection through cross-platform applications. *Proceedings of the Network and Distributed System Security Symposium*. NDSS 2013, 20th Annual Network and Distributed System Security Symposium, San Diego, CA. <http://www.ndss-symposium.org/ndss2013/ndss-2013-programme/comparing-mobile-privacy-protection-through-cross-platform-applications/>

- Helmond, A. (2015). The platformization of the web: Making web data platform ready. *Social Media and Society*, 1(2). <https://doi.org/10.1177/2056305115603080>
- IBM Cloud Education. (2021, July 13). SDK versus API: What's the difference? *IBM Think*. <https://www.ibm.com/cloud/blog/sdk-vs-api>
- IPATool. (n.d.). *Ipatool* [Repository]. Github. <https://github.com/majd/ipatool>
- Kitchin, R., & Lauriault, T. (2014). *Towards critical data studies: Charting and unpacking data assemblages and their work* (2474112). SSRN Electronic Journal. <https://papers.ssrn.com/abstract=2474112>
- Kollnig, K., Binns, R., Van Kleek, M., Lyngs, U., Zhao, J., Tinsman, C., & Shadbolt, N. (2021). Before and after GDPR: Tracking in mobile apps. *Internet Policy Review*, 10(4). <https://doi.org/10.14763/2021.4.1611>
- Kollnig, K., Shuba, A., Binns, R., Van Kleek, M., & Shadbolt, N. (2022). Are iPhones really better for privacy? A comparative study of iOS and Android apps. *Proceedings on Privacy Enhancing Technologies*, 2, 6–24. <https://doi.org/10.2478/popets-2022-0033>
- Kollnig, K., Shuba, A., Van Kleek, M., Binns, R., & Shadbolt, N. (2022). Goodbye tracking? Impact of iOS app tracking transparency and privacy labels. *Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency*, 508–520. <https://doi.org/10.1145/3531146.3533116>
- Lai, S. S., & Flensburg, S. (2021). Invasive species of the app ecosystem: Exploring the political economy of mobile communication. *International Journal of Communication*, 15. <https://ijoc.org/index.php/ijoc/article/view/16906>
- Law, J. (1990). Power, discretion and strategy. *The Sociological Review*, 38(1), 165–191. <https://doi.org/10.1111/j.1467-954X.1990.tb03352.x>
- Libimobiledevice. (n.d.). *Home*. <https://libimobiledevice.org/>
- Lomborg, S., Helles, R., & Lai, S. S. (2023). Digital tracking and infrastructural power. In S. Lindgren (Ed.), *Handbook of critical studies of artificial intelligence* (pp. 354–366). Edward Elgar Publishing. <https://doi.org/10.4337/9781803928562.00038>
- Mann, M. (1984). The autonomous power of the state: Its origins, mechanisms and results. *European Journal of Sociology*, 25(2), 185–213. <https://doi.org/10.1017/S0003975600004239>
- Mansell, R., & Plantin, J.-C. (2022). Imagining 5G networks: Infrastructure and public accountability. *International Journal of Communication*, 16. <https://ijoc.org/index.php/ijoc/article/view/18004>
- Marsden, C. T., & Brown, I. (2023). App stores, antitrust and their links to net neutrality: A review of the European policy and academic debate leading to the EU Digital Markets Act. *Internet Policy Review*, 12(1). <https://doi.org/10.14763/2023.1.1676>
- Meta. (n.d.). *Facebook SDK for Android*. Meta for Developers. <https://developers.facebook.com/docs/android/>
- Nieborg, D. B., & Poell, T. (2018). The platformization of cultural production: Theorizing the contingent cultural commodity. *New Media & Society*, 20(11), 4275–4292. <https://doi.org/10.1177/1461444818769694>
- noyb. (2022, January 13). Austrian DSB: EU-US data transfers to Google Analytics illegal. *noyb News*. <https://noyb.eu/en/austrian-dsb-eu-us-data-transfers-google-analytics-illegal>

Olifent, L. (2023, October 31). Kommune fanget i ulovlige it-kontrakter: Borgernes data bruges til reklamer [Municipality caught in illegal IT contracts: Citizen data used for advertising]. *ComplianceTech*. <https://pro.ing.dk/compliancetek/artikel/kommune-fanget-i-ulovlige-it-kontrakter-borgernes-data-bruges-til-reklamer>

Otto, E. I. (In press). Brokering data markets: The agentic power of app-builders at the edge of platforms. In A. M. Thorhauge, A. L. Gregersen, E. I. Otto, J. Ørmen, & M. A. Pedersen (Eds.), *The economic lives of platforms: Rethinking the political economy of digital markets*. Bristol University Press.

Plantin, J.-C., Lagoze, C., Edwards, P. N., & Sandvig, C. (2018). Infrastructure studies meet platform studies in the age of Google and Facebook. *New Media & Society*, 20(1), 293–310. <https://doi.org/10.1177/1461444816661553>

Poell, T., Nieborg, D., & van Dijck, J. (2019). Platformisation. *Internet Policy Review*, 8(4). <https://doi.org/10.14763/2019.4.1425>

Powell, A. B. (2021). *Undoing optimization. Civic action in smart cities*. Yale University Press.

Pybus, J., & Coté, M. (2022). Did you give permission? Datafication in the mobile ecosystem. *Information, Communication & Society*, 25(11), 1650–1668. <https://doi.org/10.1080/1369118X.2021.1877771>

Pybus, J., & Coté, M. (2024). Super SDKs: Tracking personal data and platform monopolies in the mobile. *Big Data & Society*, 11(1). <https://doi.org/10.1177/20539517241231270>

Ravnås, O. A. V. (2023, March 24). *Getting started: Welcome*. Frida. <https://frida.re/docs/home/>

Rogers, R. (2013). *Digital methods*. The MIT Press. <https://doi.org/10.7551/mitpress/8718.001.0001>

Sentry Documentation. (n.d.). *Sentry for iOS*. <https://docs.sentry.io/platforms/apple/guides/ios/>

Unity. (n.d.). *Welcome to Unity Ads*. Unity Documentation. <https://docs.unity.com/ads/en/manual/UnityAdsHome>

van Dijck, J., Nieborg, D., & Poell, T. (2019). Reframing platform power. *Internet Policy Review*, 8(2). <https://doi.org/10.14763/2019.2.1414>

van Dijck, J., Poell, T., & de Waal, M. (2018). *The platform society*. Oxford University Press. <https://doi.org/10.1093/oso/9780190889760.001.0001>

Van Kleek, M., Liccardi, I., Binns, R., Zhao, J., Weitzner, D. J., & Shadbolt, N. (2017). Better the devil you know: Exposing the data sharing practices of smartphone apps. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 5208–5220. <https://doi.org/10.1145/3025453.3025556>

Weltevrede, E., & Jansen, F. (2019). Infrastructures of intimate data: Mapping the inbound and outbound data flows of dating apps. *Computational Culture*, 7. <http://computationalculture.net/infrastructures-of-intimate-data-mapping-the-inbound-and-outbound-data-flows-of-dating-apps/>

Published by



ALEXANDER VON HUMBOLDT  
INSTITUTE FOR INTERNET  
AND SOCIETY

in cooperation with



CREATE



centre  
— internet  
et —  
societe



R&amp;I

IN3

Internet  
interdisciplinary  
Institute

Universitat Oberta de Catalunya



UNIVERSITY OF TARTU  
Johan Skytte Institute of  
Political Studies