**Report: Out of control**

14. januar, 2020

In this report, we demonstrate how every time we use our phones, a large number of shadowy entities that are virtually unknown to consumers are receiving personal data about our interests, habits, and behaviour.

As we move around on the internet and in the real world, we are being continually tracked and profiled for the purpose of showing targeted advertising. In this report, we demonstrate how every time we use our phones, a large number of shadowy entities that are virtually unknown to consumers are receiving personal data about our interests, habits, and behaviour.



Illustrasjon: Forbrukerrådet

The actors, who are part of what we call the digital marketing and adtech industry, use this information to track us over time and across devices, in order to create comprehensive profiles about individual consumers. In turn, these profiles and groups can be used to personalize and target advertising, but also for other purposes such as discrimination, manipulation, and exploitation. Although the adtech industry operates across different media such as websites, smart devices, and mobile apps, we chose to focus on adtech in apps.

In order to expose how large parts of this vast industry works, we commissioned the cybersecurity company Mnemonic to perform a technical analysis of the data traffic from ten popular mobile apps. Because of the scope of tests, size of the third parties that were observed receiving data, and popularity of the apps, we regard the findings from these tests to be representative of widespread practices in the adtech industry.

[Report: Out of Control](https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf) [Technical report – Out of Control](https://fil.forbrukerradet.no/wp-content/uploads/2020/01/mnemonic-security-test-report-v1.0.pdf)



Øyvind H. Kaldestad

Pressekontakt / Kommunikasjonsrådgiver

(+47) 480 82 619

ohk@forbrukerradet.no

[Abonner på vårt nyhetsvarsel](https://www.forbrukerradet.no/nyhetsvarsling)

**TECHNICAL REPORT**

**“OUT OF CONTROL” – A REVIEW OF DATA SHARING BY POPULAR MOBILE APPS**

Norwegian Consumer Council

**Place** Oslo

**Date** 14.01.2020

**Version** 1.0

**Authors** Andreas Claesson and Tor E. Bjørstad

“Out of Control” – A review of data sharing by popular mobile apps - Norwegian Consumer Council mnemonic

CLASSIFICATION: PUBLIC 2

**Report summary**

**Introduction**

As part of an ongoing collaboration with the digital consumer rights team at the Norwegian Consumer Council (NCC), mnemonic researchers have carried out an in-depth investigation into how mobile applications share data with third parties for advertising purposes. The analysis has covered a selection of 10 popular mobile applications on the Android platform.

The purpose of the testing has been to increase our understanding of the mobile advertising ecosystem. In particular, we have aimed to identify some of the main actors collecting user data from our sample set of apps, understand the type and frequency of data flows, and examine the specific information that is being transmitted.

A key motivation for this project has been that data collection, sharing, and processing within the advertising industry on mobile platforms is poorly understood by the general public, policy-makers, and the tech community. One of our main goals has been to help clarify this topic.

All the apps have been analysed in mnemonic’s mobile testing lab, where we have set up infrastructure to monitor and capture communications from our test device. The project has been carried out between May and December 2019, with the majority of testing in July and August.

From our testing, we have collected a large amount of mobile traffic data, while working without any inside knowledge of the data collection ecosystems. The vast volumes, as well as the nature of black-box analysis, has made it hard to interpret the data and get a complete picture of the situation. This report documents data collection and sharing practices which appear highly problematic in terms of data privacy and consent. However, these findings are by no means exhaustive. We hope that this report may serve as the beginning of a debate on mobile advertising practices, rather than the final word.

**Summary of findings**

Some of the key findings in this report are:

1. All apps tested share user data with multiple third parties, and all but one share data beyond the device advertising ID. This includes information such as the IP address and GPS position of the user, personal attributes such as gender and age, and app activities such as GUI events. In many cases, this information can be used to infer attributes such as sexual orientation or religious belief.

2. The **Grindr** app shares detailed user data with a very large number of third parties, including IP address, GPS location, age, and gender. By using **MoPub** as a mediator, the data sharing is highly opaque as neither the third parties nor the information transmitted are not known in advance. We have also seen that **MoPub** can enrich the data that is shared with other parties dynamically.

3. The **Perfect365** app shares user data with a very large number of third parties, including attributes such as advertising ID, IP address, and GPS position. One could almost say that the app appears to be built to collect and share as much user data as possible.

4. The **MyDays** app shares the user’s GPS location with multiple parties, and the **OkCupid** app shares detailed personal questions and answers with **Braze**.

During testing, more than **88.000 web requests** made by the apps were logged and analysed, covering **216 unique domains** and at least **135 third parties** within the advertising space.

“Out of Control” – A review of data sharing by popular mobile apps - Norwegian Consumer Council mnemonic

CLASSIFICATION: PUBLIC 3

Figure 1 visualises the data flows observed for companies who receive data from multiple apps.

*Figure 1. Advertising companies receiving data from multiple apps*

**About mnemonic**

mnemonic helps businesses manage their security risks, protect their data and defend against cyber threats. Our expert team of security consultants, product specialists, threat researchers, incident responders and ethical hackers, combined with our Argus security platform ensures we stay ahead of advanced cyberattacks and protect our customers from evolving threats.

Acknowledged by Gartner as a notable vendor in delivering Managed Security Services, threat intelligence and advanced targeted attack detection, we are among the largest IT security service providers in Europe, the preferred security partner of the region’s top companies and a trusted source of threat intelligence to Europol and other law enforcement agencies globally.

With intelligence-driven managed security services, 185+ security experts and partnerships with leading security vendors, mnemonic enables businesses to stay secure and compliant while reducing costs.

This is the second major collaboration between the NCC and mnemonic, the first being the #WatchOut1 investigation into the cybersecurity of smart watches for children in 2017.

1 Published as https://www.forbrukerradet.no/side/significant-security-flaws-in-smartwatches-for-children/ and https://mnemonic.no/watchout on October 18th, 2017

“Out of Control” – A review of data sharing by popular mobile apps - Norwegian Consumer Council mnemonic

CLASSIFICATION: PUBLIC 4

Table of Contents

1 Introduction .............................................................................................................................8

1.1 Introduction to the report ................................................................................................8

1.2 Apps tested by mnemonic ..............................................................................................9

1.3 Test scope and boundaries ............................................................................................9

1.4 Structure of the report ..................................................................................................11

1.5 Acknowledgements ......................................................................................................11

2 Summary of findings .............................................................................................................12

2.1 Scenarios and problem areas ......................................................................................12

2.2 Summary of findings per app .......................................................................................13

2.3 Statistics, facts, and figures ..........................................................................................14

2.3.1 General information ..................................................................................................14

2.3.2 Overall data sharing .................................................................................................15

2.3.3 Use of third party SDKs ............................................................................................16

2.3.4 Commonly observed domains ..................................................................................18

3 Detailed findings and observations .......................................................................................20

3.1 Introduction ...................................................................................................................20

3.1.1 Data elements ..........................................................................................................20

3.1.2 Interaction types .......................................................................................................22

3.2 Grindr ...........................................................................................................................23

3.2.1 Grindr’s use of MoPub for ad mediation ...................................................................23

3.2.2 Direct interactions between Grindr and other third parties .......................................29

3.2.3 A note on gender in Grindr .......................................................................................30

3.2.4 Traffic from Grindr to Smaato, and use of the IAB consent string ............................31

3.2.5 Traffic from Grindr to Braze ......................................................................................32

3.3 Perfect365 ....................................................................................................................34

3.3.1 General observations ...............................................................................................34

3.3.2 Location sharing from the Perfect365 app to third parties ........................................35

3.3.3 Vungle and the unknown GDPR consent .................................................................36

3.3.4 Unencrypted traffic from Perfect365 to third parties .................................................37

3.3.5 Perfect365 interaction with FluxLoop (Pinch) and Unacast ......................................38

3.4 MyDays ........................................................................................................................40

3.4.1 General observations ...............................................................................................40

3.4.2 Data transmission from MyDays to Placed ...............................................................40

3.4.3 Location data sharing from MyDays to Neura and Placer ........................................42

“Out of Control” – A review of data sharing by popular mobile apps - Norwegian Consumer Council mnemonic

CLASSIFICATION: PUBLIC 5

3.5 OkCupid .......................................................................................................................46

3.5.1 General observations ...............................................................................................46

3.5.2 Data transmissions from OkCupid to Braze .............................................................48

3.6 My Talking Tom 2 .........................................................................................................52

3.6.1 General observations ...............................................................................................52

3.6.2 My Talking Tom 2’s use of IQzone for ad mediation ................................................54

3.7 Muslim: Qibla finder ......................................................................................................57

3.7.1 General observations ...............................................................................................57

3.8 Tinder ...........................................................................................................................60

3.8.1 General observations ...............................................................................................60

3.8.2 User data transmission from Tinder to LeanPlum and AppsFlyer ............................60

3.9 Clue ..............................................................................................................................64

3.9.1 General observations ...............................................................................................64

3.10 Happn ...........................................................................................................................65

3.10.1 General observations ...........................................................................................65

3.11 Wave Keyboard ............................................................................................................66

3.12 The effect of opting out of ad tracking ..........................................................................67

3.13 Other noteworthy observations ....................................................................................70

3.13.1 Observations regarding public IP address ............................................................70

3.13.2 Unattributed traffic to Tutela .................................................................................72

3.13.3 Unattributed traffic to AreaMetrics ........................................................................72

3.13.4 Correlating traffic from multiple sources – AppsFlyer example ............................73

4 Test environment and methodology ......................................................................................75

4.1 Summary ......................................................................................................................75

4.2 Test device description .................................................................................................75

4.3 Test environment description .......................................................................................76

4.4 Test protocol .................................................................................................................76

4.5 Known limitations of technical setup.............................................................................78

4.6 Personal data ...............................................................................................................78

4.7 Generality of results .....................................................................................................79

5 About the report ....................................................................................................................80

5.1 Test execution ..............................................................................................................80

5.2 Document version control .............................................................................................80

5.3 Project timeline .............................................................................................................80

Appendix A: List of apps and versions .........................................................................................82

Appendix B: List of identified third parties ....................................................................................83

“Out of Control” – A review of data sharing by popular mobile apps - Norwegian Consumer Council mnemonic

CLASSIFICATION: PUBLIC 6

List of tables and figures

**Tables**

Table 1. List of apps tested by mnemonic ......................................................................................9

Table 2. Summary of findings per app .........................................................................................14

Table 3. Overview of data sharing for each app ..........................................................................16

Table 4. List of third-party SDKs integrated in the apps ...............................................................17

Table 5. Most frequently observed third parties, in terms of number of requests sent by the apps, as identified by mnemonic ............................................................................................................19

Table 6. List of typical data elements collected ............................................................................22

Table 7. Initial request from the Grindr app to MoPub. The request body, formatted and trimmed for legibility, contains GPS position, device advertising ID, and user data (highlighted) ..............24

Table 8. Response (excerpted) from MoPub to the request in Table 7, showing how MoPub instructs the app to request a resource from secure.adnxs.com (highlighted). Parameters sent to AppNexus includes the app bundle name, external IP address, and device advertising ID ........25

Table 9. Request from the Grindr app to AppNexus, containing parameters previously specified by MoPub ...................................................................................................................................26

Table 10. Overview of third-party companies receiving data from the Grindr app that appear to be part of MoPub’s mediation network .........................................................................................28

Table 11. Request parameters sent from the Grindr app to OpenX, as part of a MoPub mediation flow .............................................................................................................................................28

Table 12. Third parties receiving data directly from the Grindr app .............................................30

Table 13. Typical request parameters sent from the Grindr app to Smaato ................................31

Table 14. Example of IAB consent string sent from the Grindr app to Smaato ............................32

Table 15. Excerpt of Consensu’s vendor list used in the consent string ......................................32

Table 16. Examples of data sent from the Grindr app to Braze: app activity, GPS location, and type of relationship .......................................................................................................................33

Table 17. Request sent from the Perfect365 app to Fysical (beaconsinspace) ...........................35

Table 18. Decoded payload sent from the Perfect365 app to Fysical / beaconsinspace .............36

Table 19. Example request from the Perfect365 app to Vungle, containing location and missing GDPR consent .............................................................................................................................37

Table 20. User data sent unencrypted from the Perfect365 app to Receptiv / Verve (mediabrix.com) ...........................................................................................................................38

Table 21. Data sent from the Perfect365 app to what we think is Unacast ..................................39

Table 22. Excerpts of data sent from the MyDays app to Placed on July 16th ............................41

Table 23. Excerpts from list of installed packages, sent from the MyDays app to Placed ...........42

Table 24. Authorization token sent from MyDays to Placed, before and after base64 decoding .42

Table 25. Request from the MyDays app to Neura on July 12th. In a separate transmission, neighbouring wifi networks were also listed in detail ....................................................................44

Table 26. Excerpts from request sent from the MyDays app to Placer on July 16th ...................45

Table 27. Data transmitted from the OkCupid app to AppsFlyer .................................................47

Table 28. Data transmitted from the OkCupid app to Facebook ..................................................47

Table 29. Data transmitted from the OkCupid app to Kochava ....................................................48

Table 30. Examples of user data and geolocation sent to Braze .................................................50

Table 31. Examples of user answers to sensitive questions in the OkCupid app, sent to Braze .51

Table 32. Requests from My Talking Tom app to PubNative, Mobfox, and Rubicon Project ......54

“Out of Control” – A review of data sharing by popular mobile apps - Norwegian Consumer Council mnemonic

CLASSIFICATION: PUBLIC 7

Table 33. Initial request sent from the My Talking Tom 2 app to IQzone .....................................54

Table 34. Response from IQzone to the My Talking Tom 2 app, showing which fields to populate in the subsequent request ............................................................................................................55

Table 35. Request sent from the My Talking Tom 2 app to MobFox, containing IP address and advertising ID ...............................................................................................................................55

Table 36. Example request from the Muslim app to Appodeal, containing the public IP address58

Table 37. Request from the Muslim app to Liftoff containing inexact location information ..........59

Table 38. Excerpt of data sent from the Tinder app to AppsFlyer (formatted for legibility) ..........61

Table 39. Excerpt of data sent from the Tinder app to LeanPlum (formatted for legibility) ..........62

Table 40. Event types transmitted from the Clue app to Amplitude .............................................64

Table 41. Data transmission from the Happn app to Google Doubleclick ....................................65

Table 42. Comparison of data sent from the Grindr app to AdColony, with and without opt-out from personalisation .....................................................................................................................68

Table 43.Comparison of data sent from the Grindr app to AppsFlyer, with and without opt-out from personalisation .....................................................................................................................69

Table 44. Request from app to find its public IP address through a public service ......................70

Table 45. Traffic from unknown mobile app to Tutela Technologies ............................................72

Table 46. Traffic from unknown mobile app to AreaMetrics .........................................................73

Table 47. Comparison of transmissions to AppsFlyer from multiple apps, selected parameters .74

Table 48. Examples of app identifiers observed in traffic .............................................................77

Table 49. Project metadata ..........................................................................................................80

Table 50. Document version control ............................................................................................80

Table 51. List of apps and versions .............................................................................................82

Table 52. List of 135 identified third parties .................................................................................93

**Figures**

Figure 1. Advertising companies receiving data from multiple apps ..............................................3

Figure 2. Illustration of SDKs that were used by multiple apps ....................................................18

Figure 3. Sequence diagram showing data transmission between Grindr, MoPub, and third party advertising networks ....................................................................................................................26

Figure 4: Sequence diagram showing the information flow between the My Talking Tom 2 app and various third-party companies, using IQzone as mediator ....................................................56

Figure 5. Transmission from the Tinder app to LeanPlum when looking for women ...................63

Figure 6. Transmission from the Tinder app to LeanPlum when looking for men ........................63

Figure 7. Transmission from the Tinder app to LeanPlum when looking for women **and** men ....63

Figure 8. A summary of how opting out of ads personalization affects data transmission from Grindr. Green means that there is an observable difference, yellow means a partial difference, and red means that there is no change. .......................................................................................67

Figure 9. Decompiled source code excerpt of the IQzone SDK, which is built into the My Talking Tom 2 app ..................................................................................................................................71

“Out of Control” – A review of data sharing by popular mobile apps - Norwegian Consumer Council mnemonic

CLASSIFICATION: PUBLIC 8

**1 Introduction**

**1.1 Introduction to the report**

mnemonic has carried out an in-depth investigation of 10 popular mobile apps, focusing on the type and amount of personal data that is being shared with third parties for advertising purposes. The purpose of the testing has been to gain knowledge about how the mobile advertising ecosystem works, in terms of data sharing and communication patterns, and document concrete examples of how user data is being collected and shared as part of app monetization.

All the testing carried out as part of this research has been done on Google’s Android platform, with apps downloaded from the Google Play store. This was a practical decision made early on in the project, based on the fact that it would require significant additional effort to cover additional platforms such as iOS, and that the Android platform has by far the highest market share in the smartphone market globally2. Another factor is that Google plays a significant role in online advertising, although this has not been a primary focus of the research.

2 Domestically in Norway, the respective market shares of Android and Apple’s iOS are estimated to be roughly equal, although precise numbers are not known to us. Globally, Android is known to have the largest market share, estimated at about 75%.

3 The NCC’s full report and additional information about the project can be obtained at https://www.forbrukerradet.no/out-of-control/

Our tests have covered 10 apps that are well-known and widely used, which were selected for analysis by the Norwegian Consumer Council. The apps cover a number of highly personal topics, such as dating, religion, and health. Chapter 1.2 provides a list of the specific apps and versions tested.

The results of our testing document that a significant degree of user data, including personal data, is being shared from the apps with third parties in the advertising or “adtech” industry. We expect that our results will be widely applicable to other people in Norway, using the same apps during the same time as the testing was carried out. We also expect that the findings are broadly generalizable within the EU / EEA. Privacy controls on the iOS platform are more stringent than on Android, but we expect that some of the findings would also apply there.

This report describes the results of the technical testing in further detail, providing evidence of our findings, as well as mnemonic’s initial analysis and evaluation. Due to the sheer volume of data, as well as the presence of some personal data related to location in the datasets, the underlying raw data from our analysis is not included as part of the report.

For additional contextual information about the mobile advertising industry, and higher-level analysis of the findings, we refer to the Norwegian Consumer Council’s technical report, *Out of Control – How consumers are exploited by the online advertising industry 3*, which is published as a companion to this work.

“Out of Control” – A review of data sharing by popular mobile apps - Norwegian Consumer Council mnemonic

CLASSIFICATION: PUBLIC 9

**1.2 Apps tested by mnemonic**

mnemonic has tested 10 popular mobile apps on the Android platform. The apps are listed and categorised in Table 1.

|  |  |  |
| --- | --- | --- |
| **App**  | **Package name**  | **Category**  |
| Grindr  | com.grindrapp.android  | Gay dating  |
| Perfect365  | com.arcsoft.perfect365  | Virtual makeup  |
| My Days  | com.chris.mydays  | Period tracker  |
| OkCupid  | com.okcupid.okcupid  | Online dating  |
| My Talking Tom 2  | com.outfit7.mytalkingtom2  | Children’s app  |
| Muslim: Qibla Finder  | com.hundred.qibla  | Muslim assistant  |
| Tinder  | com.tinder  | Online dating  |
| Clue  | com.clue.android  | Period tracker  |
| Happn  | com.ftw\_and\_co.happn  | Online dating  |
| Wave Keyboard  | com.wave.keyboard  | Keyboard themes  |

**Complaints against Grindr and five third party companies**

14. januar, 2020

The Norwegian Consumer Council is filing formal complaints against Grindr and five companies that were receiving personal data through the app;  Twitter`s MoPub, AT&T’s AppNexus, OpenX, AdColony and Smaato.

The complaints are a part of the project «Out of control» and are directed to the Norwegian Data Protection Agency for breaches of the General Data Protection Regulation (GDPR).

[Complaint 1. against Grindr, Twitter MoPub, AppNexus and OpenX](https://fil.forbrukerradet.no/wp-content/uploads/2020/01/20200114-complaint-grindr-twitter-mopub-appnexus-openx.pdf) [Complaint 2. against Grindr and AdColony](https://fil.forbrukerradet.no/wp-content/uploads/2020/01/20200114-complaint-grindr-adcolony.pdf) [Complaint against 3. Grindr and Smaato](https://fil.forbrukerradet.no/wp-content/uploads/2020/01/20200114-complaint-grindr-smaato.pdf)