Unified Patent Court
Einheitliches Patentgericht
Juridiction unifiée du brevet

Düsseldorf Local Division
UPC_CFI_26/2024

Decision

of the Court of First Instance of the Unified Patent Court
delivered on 30 July 2025
concerning EP 3 110 069 B1

Headnotes:

> The Court can reject a new line of arguments pursuant to R. 9.2 RoP in a case where the issue has been raised from the outset and the new argument is based on completely different passages of a lengthy document. Neither the Court nor the other party may be forced to deal with it from scratch. This undermines the concept of the front-loaded procedure established by the Rules of Procedure.

Keywords:

Rule 9.2 RoP; added-matter

CLAIMANT:

1. **Headwater Research LLC**, represented by the Member of the Managing Board, Dr Gregory Raleigh, 110 North College Avenue, Suite 1116, Tyler, TX 75702, USA

all Claimants represented by: Dr Michael Schneider and Jochen Ehlers, EISENFÜHR SPEISER, Gollierstraße 4, 80339 Munich, Germany

electronic address for service: mschneider@eisenfuhr.com

DEFENDANTS:

1. **Samsung Electronics GmbH**, represented by its CEO Man Young Kim, Am Kronberger Hang 6, 65824 Schwalbach/Taunus, Germany

2. **Samsung Electronics France, S.A.S.**, represented by its CEO Menno Van Den Berg, 6 Rue Fructidor, CS 2003, 93400 Saint-Ouen-Sur-Seine, France

3. **Samsung Electronics Benelux B.V.**, represented by its CEOs Choon Young Park, Ji Hoon Lee and Jeewook Kim, Evert van de Beekstraat 310, 1118 CX Schiphol, The Netherlands

4. **Samsung Electronics Co. Ltd.**, represented by its Chairman Mr. Lee Jae-yong, 129, Samseong-ro Yeongtong-gu Suwon-si, Gyeonggi-do 16677, Republic of Korea

all Defendants represented by: Dr Martin Köhler, Hoyng ROKH Monegier, Steinstraße 20, 40212 Düsseldorf, Germany

electronic address for service: martin.koehler@hoyngrokh.com

PATENT AT ISSUE:

European Patent No. 3 110 069 B1

PANEL/DIVISION:

Panel of the Local Division in Düsseldorf

DECIDING JUDGES:

This decision is issued by Presiding Judge Thomas, by the legally qualified judge Dr Thom acting as judge-rapporteur, the legally qualified judge Agergaard and the technically qualified judge Augarde.

LANGUAGE OF THE PROCEEDINGS: English

SUBJECT: Infringement action and counterclaim for revocation

DATE OF ORAL HEARING: 17 June 2025

SHORT SUMMARY OF FACTS:

1. The Claimant is (at least one of the) proprietor(s) of the European patent EP 3 110 069 B1 (Exhibit ES 1; in the following: patent in suit). The patent in suit derives from the European patent application number 15177549.9, which is a first-generation divisional application of the European patent application with the application number 11787024.6. The latter is the regional phase of the international patent application PCT/US2011/000937, which was filed on 25 May 2011 and published under publication number WO 2011/149532 A1. The patent in suit claims priority to US patent applications 61/348,022 of 25 May 2010, 61/381,159 of 9 September 2010 and 61/435,564 of 24 January 2011. The patent in suit was granted in English with effect in Germany, the Netherlands and France. The mention of the grant of the patent in suit was published on 16 August 2017.

2. There are no opposition proceedings pending before the EPO. The patent in suit is in force.

3. Claim 1 of the patent in suit reads as follows:

> *"A wireless end-user device (100), comprising:*
>
> *a processor (115);*
>
> *a wireless wide area network, WWAN, modem (1812) to communicate data for network service usage activities between the device and a WWAN, when connected to a WWAN;*
>
> *a wireless local area network, WLAN, modem (1813) to communicate data for network service usage activities between the device and a WLAN, when connected to a WLAN;*
>
> *a computer-readable storage medium storing instructions that, when provided to the processor (115), cause the processor (115) to*
>
> *determine, for a first device application whether the application is running in a background state or in a foreground state, and control, via an application program interface, API, application access for network service, usage activities provided through the WWAN modem (1812) and the WLAN modem (1813), to, based on a first traffic control policy, selectively block and allow access by the first device application to at least one of the WWAN and WLAN modems (1812, 1813),*
>
> *wherein the access is selectively blocked based on a determination that the first device application is running in a background state, and*
>
> *wherein the access is selectively allowed based on a determination that the first device application is running in a foreground state."*

4. With regard to the wording of claims 2, 3, 4, 8 and 10, reference is made to the patent in suit.

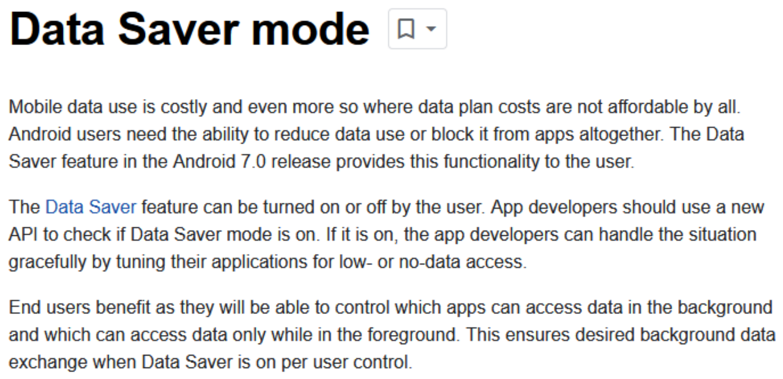
5. The Claimant holds patents in the electronic sector and its business is based inter alia on creating license revenue.

6. In […] became an employee of […]. […] (hereinafter: Inventor (2)) worked with inventor (1) at […] and also [….] as an employee [….]. As a condition of employment at [….] each of the inventors, inventor (1) and inventor (2), entered into a patent assignment agreement […]. Inventor (1) left […] on […], Inventor (2) left […] on […]. Inventor (1) founded the Claimant. […]

7. Defendant 4) is a global electronics company and belongs to the Samsung Group based in South Korea. Defendant 1) is the German sales subsidiary of Defendant 4). Defendant 2) is its French sales subsidiary and Defendant 3) is the Dutch sales subsidiary of Defendant 4). Defendant 1) to 3) offer and distribute the alleged infringing smartphones in Germany, France and the Netherlands via national sub-webpages https://www.samsung.com/de/, https://www.samsung.com/fr/ and https://www.samsung.com/nl/. Defendant 4) signs responsible for the content of the operating instructions of the alleged infringing smartphones distributed by Defendants 1) to 3) (exhibit ES 12).

8. Claimant directs its infringement action against all mobile devices bearing the trade mark "Samsung", which have a processor and a modem for mobile communication and which are operated with the System Android 7 ("Android Nougat") or higher (hereinafter also referred to as "attacked embodiment"). The Android system comprises a Data Saver functionality, which is at the centre of the dispute in question.

9. The advantages and effects of that functionality are generally described on the source.android.com website for Android developers which is shown in the following, slightly reduced excerpt taken from the Statement of claim.



Data Saver mode

Mobile data use is costly and even more so where data plan costs are not affordable by all. Android users need the ability to reduce data use or block it from apps altogether. The Data Saver feature in the Android 7.0 release provides this functionality to the user.

The Data Saver feature can be turned on or off by the user. App developers should use a new API to check if Data Saver mode is on. If it is on, the app developers can handle the situation gracefully by tuning their applications for low- or no-data access.

End users benefit as they will be able to control which apps can access data in the background and which can access data only while in the foreground. This ensures desired background data exchange when Data Saver is on per user control.

10. The first aspect of the Data Saver Functionality controls the data consumption of apps by

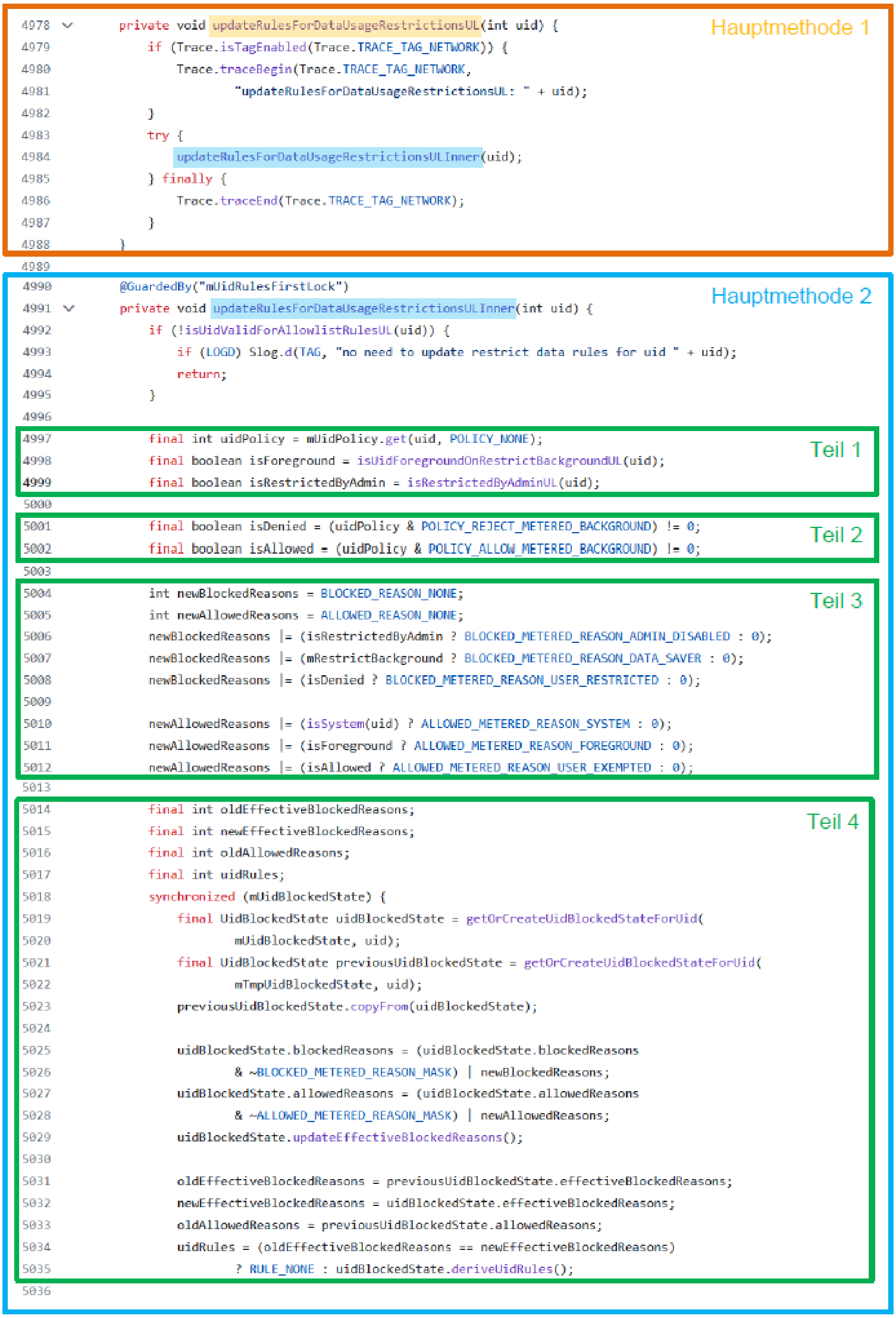
> **Option #1´**: deactivating the background data for all apps with the “data saver mode” in order to save data volume in a mobile network.
>
> Two other aspects of the Data Saver Functionality involve options for the user to block network access for specific apps running in a background state. These include
>
> **Option #2’**: The user requests to block network access for a specific app running in a background state, even when the data saver mode is deactivated; and
>
> **Option #3’**: The user requests to allow network access for a specific app running in a background state, even when the data saver mode is activated.

11. These options are implemented by the *NetworkPolicyManager API* and the *ConnectivityManager API* on Android:

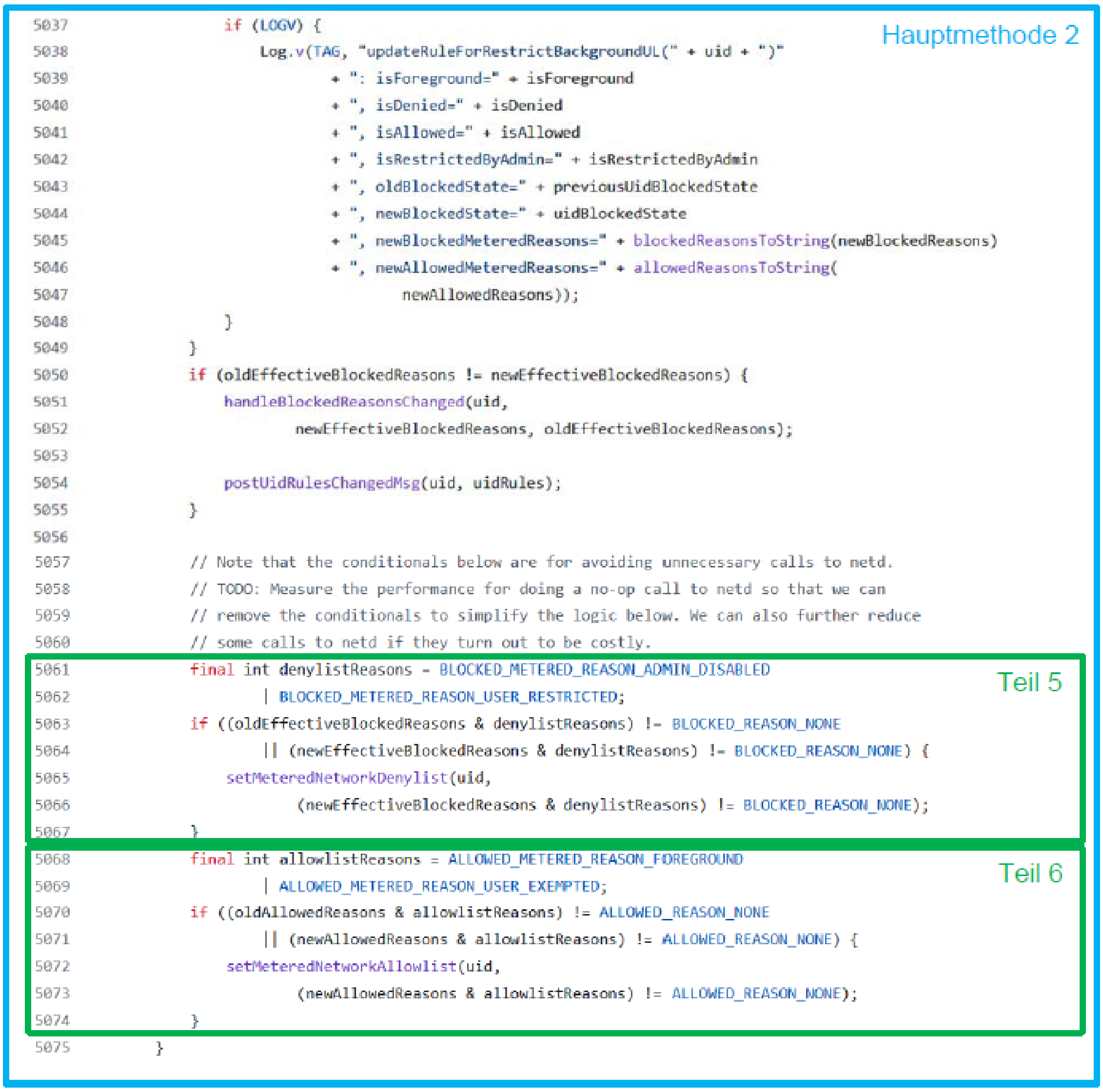
12. The *NetworkPolicyManager API* within the Android operating system is responsible, among other things, for updating internal and external rules for allowing or blocking access to an available network. The *ConnectivityManager API* is responsible for network monitoring and connection management to networks such as WWAN or WLAN within the Android operating system. The Android code implements the Data Saver functionality centrally with the two

methods *updateRulesForDataUsageRestrictionsUL* ("first main method") and *updateRulesForDataUsageRestrictionsULInner* ("second main method") of the *NetworkPolicyManagerService*. The *NetworkPolicyManagerService* can be used to assign policies to individual or all apps that control their access rights to mobile networks and, in particular, whether an app that is in a background state is allowed to access a mobile network or not.

13. The following slightly reduced picture from Exhibit ES16 (colouring was made by the Claimant) shows the Data Saver Code of the attacked embodiment:



```
private void updateRulesForDataUsageRestrictionsUL(int uid) {
    if (Trace.isTagEnabled(Trace.TRACE_TAG_NETWORK)) {
        Trace.traceBegin(Trace.TRACE_TAG_NETWORK,
                "updateRulesForDataUsageRestrictionsUL: " + uid);
    }
    try {
        updateRulesForDataUsageRestrictionsULInner(uid);
    } finally {
        Trace.traceEnd(Trace.TRACE_TAG_NETWORK);
    }
}

@GuardedBy("mUidRulesFirstLock")
private void updateRulesForDataUsageRestrictionsULInner(int uid) {
    if (!isUidValidForAllowlistRulesUL(uid)) {
        if (LOGD) Slog.d(TAG, "no need to update restrict data rules for uid " + uid);
        return;
    }

    final int uidPolicy = mUidPolicy.get(uid, POLICY_NONE);
    final boolean isForeground = isUidForegroundOnRestrictBackgroundUL(uid);
    final boolean isRestrictedByAdmin = isRestrictedByAdminUL(uid);

    final boolean isDenied = (uidPolicy & POLICY_REJECT_METERED_BACKGROUND) != 0;
    final boolean isAllowed = (uidPolicy & POLICY_ALLOW_METERED_BACKGROUND) != 0;

    int newBlockedReasons = BLOCKED_REASON_NONE;
    int newAllowedReasons = ALLOWED_REASON_NONE;
    newBlockedReasons |= (isRestrictedByAdmin ? BLOCKED_METERED_REASON_ADMIN_DISABLED : 0);
    newBlockedReasons |= (mRestrictBackground ? BLOCKED_METERED_REASON_DATA_SAVER : 0);
    newBlockedReasons |= (isDenied ? BLOCKED_METERED_REASON_USER_RESTRICTED : 0);

    newAllowedReasons |= (isSystem(uid) ? ALLOWED_METERED_REASON_SYSTEM : 0);
    newAllowedReasons |= (isForeground ? ALLOWED_METERED_REASON_FOREGROUND : 0);
    newAllowedReasons |= (isAllowed ? ALLOWED_METERED_REASON_USER_EXEMPTED : 0);

    final int oldEffectiveBlockedReasons;
    final int newEffectiveBlockedReasons;
    final int oldAllowedReasons;
    final int uidRules;
    synchronized (mUidBlockedState) {
        final UidBlockedState uidBlockedState = getOrCreateUidBlockedStateForUid(
                mUidBlockedState, uid);
        final UidBlockedState previousUidBlockedState = getOrCreateUidBlockedStateForUid(
                mTmpUidBlockedState, uid);
        previousUidBlockedState.copyFrom(uidBlockedState);

        uidBlockedState.blockedReasons = (uidBlockedState.blockedReasons
                & ~BLOCKED_METERED_REASON_MASK) | newBlockedReasons;
        uidBlockedState.allowedReasons = (uidBlockedState.allowedReasons
                & ~ALLOWED_METERED_REASON_MASK) | newAllowedReasons;
        uidBlockedState.updateEffectiveBlockedReasons();

        oldEffectiveBlockedReasons = previousUidBlockedState.effectiveBlockedReasons;
        newEffectiveBlockedReasons = uidBlockedState.effectiveBlockedReasons;
        oldAllowedReasons = previousUidBlockedState.allowedReasons;
        uidRules = (oldEffectiveBlockedReasons == newEffectiveBlockedReasons)
                ? RULE_NONE : uidBlockedState.deriveUidRules();
```



```
5037                if (LOGV) {
5038                    Log.v(TAG, "updateRuleForRestrictBackgroundUL(" + uid + ")"
5039                            + ": isForeground=" + isForeground
5040                            + ", isDenied=" + isDenied
5041                            + ", isAllowed=" + isAllowed
5042                            + ", isRestrictedByAdmin=" + isRestrictedByAdmin
5043                            + ", oldBlockedState=" + previousUidBlockedState
5044                            + ", newBlockedState=" + uidBlockedState
5045                            + ", newBlockedMeteredReasons=" + blockedReasonsToString(newBlockedReasons)
5046                            + ", newAllowedMeteredReasons=" + allowedReasonsToString(
5047                                    newAllowedReasons));
5048                }
5049            }
5050            if (oldEffectiveBlockedReasons != newEffectiveBlockedReasons) {
5051                handleBlockedReasonsChanged(uid,
5052                        newEffectiveBlockedReasons, oldEffectiveBlockedReasons);
5053
5054                postUidRulesChangedMsg(uid, uidRules);
5055            }
5056
5057            // Note that the conditionals below are for avoiding unnecessary calls to netd.
5058            // TODO: Measure the performance for doing a no-op call to netd so that we can
5059            // remove the conditionals to simplify the logic below. We can also further reduce
5060            // some calls to netd if they turn out to be costly.
5061            final int denylistReasons = BLOCKED_METERED_REASON_ADMIN_DISABLED
5062                    | BLOCKED_METERED_REASON_USER_RESTRICTED;
5063            if ((oldEffectiveBlockedReasons & denylistReasons) != BLOCKED_REASON_NONE
5064                    || (newEffectiveBlockedReasons & denylistReasons) != BLOCKED_REASON_NONE) {
5065                setMeteredNetworkDenylist(uid,
5066                        (newEffectiveBlockedReasons & denylistReasons) != BLOCKED_REASON_NONE);
5067            }
5068            final int allowlistReasons = ALLOWED_METERED_REASON_FOREGROUND
5069                    | ALLOWED_METERED_REASON_USER_EXEMPTED;
5070            if ((oldAllowedReasons & allowlistReasons) != ALLOWED_REASON_NONE
5071                    || (newAllowedReasons & allowlistReasons) != ALLOWED_REASON_NONE) {
5072                setMeteredNetworkAllowlist(uid,
5073                        (newAllowedReasons & allowlistReasons) != ALLOWED_REASON_NONE);
5074            }
5075        }
```

14. The most important task of the first method *updateRulesForDataUsageRestrictionsUL* (orange block) is to update internal rules and the external rules of a firewall function, which ultimately blocks or allows requests from an app to a network. In addition, the first main method in the orange block is used to call the second, much more extensive main method *updateRulesForDataUsageRestrictionsULInner*.

15. Part of the second main method in the code are option #1´ in part 3 and option #2´and option #3´ in part 2:

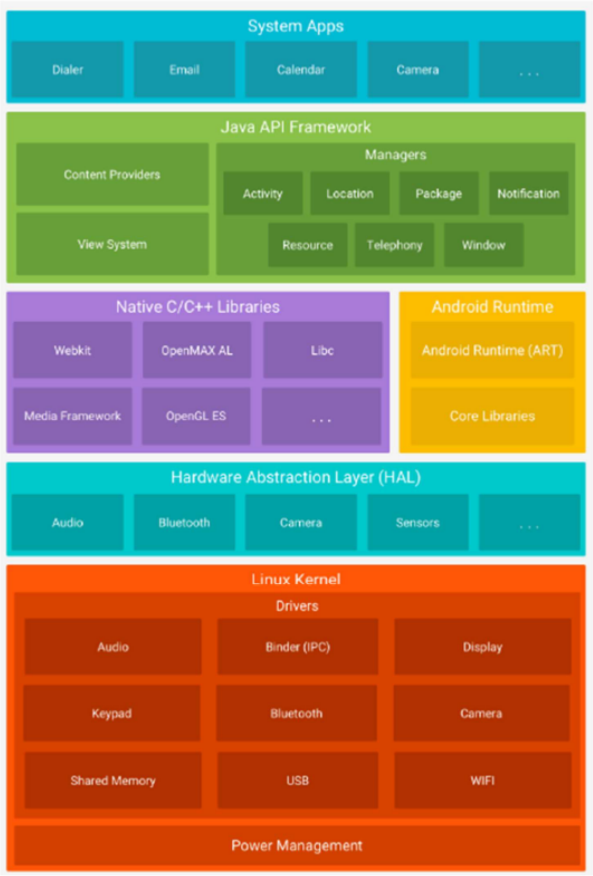
    If the user activates the data saver mode (**option #1’**), the variable *mRestrictBackground* (code part 3, line 5007) is set to "1". (If the data saving mode is deactivated, the value of the variable mRestrictBackground is "0"). The name part "RestrictBackground" already expresses that background data should be restricted (more precisely: blocked) in data saving mode;

    if the user prohibits a specific app from accessing background data (**option #2’**), a constant POLICY_REJECT_METERED_BACKGROUND (code part 2, line 5001) is set for this app. This constant is also referred to as the "app policy" (uidPolicy), as it specifies ("policy") that chargeable data traffic in the background ("metered background") should be rejected ("reject").

If the user allows a specific app unrestricted access to background data while data saving mode is activated (**option #3'**), the constant POLICY_ALLOW_ METERED_BACKGROUND (code part 2, line 5002) is set as the "app policy" for this app. This policy specifies that data traffic of the app in the background ("metered background") should be permitted ("allow").

16. The two methods enforce certain "policies" provided by the *NetworkPolicyManager*, which can be attributed to specific apps either by the system or by the user.

17. The *NetworkPolicyManager* and the *Connectivity Manager* are assigned to the "Manager" category in the JAVA API Framework layer (green box, see below slightly reduced figure 6 taken from the Statement of Defence) of the layer architecture of the Android operation system. The JAVA API Framework provides so-called Java classes implementing specific services which are provided to the applications.



18. The "methods", i.e. the software commands with which the *NetworkPolicyManager API* assigns device applications policies for accessing mobile data networks or modifies them, are stored in the *NetworkPolicyManagerService* subcomponent. *The NetworkPolicyManager* continuously checks for each app whether a process currently being executed by it is assigned to a foreground state or a background state. If the state of the process is assessed as a foreground process, the app is in the foreground state accordingly. Conversely, the app runs in the background if the status of the process of an app is evaluated as a background

process. The continuous, app-specific check of the app status is possible because each app on an Android device is assigned a unique identifier, known as a "UID" (User Identifier), which is permanent and unique throughout the system.

19. The *isUidForegroundOnRestrictBackground* method differentiates between the foreground and background state using a further variable *procState* (short for "process state"). This is because each app can initiate different processes whose state is described by the procState variable. In contrast to the static nature of the UID, which is permanently assigned to an app, *procState* is a dynamic property, meaning a running process, that changes depending on the current status and activity of the process initiated by the app. If the Data Saver functionality is activated and an app has a *procState* with a value between -1 and 5, Android considers this app to be running in the foreground state; if the value of the *procState* variable is 6 or higher, the app is considered to be running in the background state.

20. The attacked embodiments regulate network access in metered networks on the Kernel level (red box in figure 6 above) on the basis of three different firewall chains:

• HAPPY BOX (allowlist)	access to modem allowed
• PENALTY BOX (denylist)	access to modem not allowed
• Data Saver	access to modem depending on Data Saver on/off

21. Depending on different circumstances, the Unique Identifiers (UIDs) of the applications are allocated exclusively to either a HAPPY BOX or a PENALTY BOX. This is communicated via the *ConnectivityManagerService* and the *NetworkPolicyManagerService* to the bandwith controller resting on the Kernel level (exhibit I-D9).

22. The “bw_controller” relies as input on certain parameters provided by the *ConnectivityManager*, the *ConnectivityService*, the N*etworkPolicyManagerService* and the *NetworkManagementService*. Based on the respective input the UID of an application is added (“add”) to or removed (“remove”) from either “UidOnMeteredNetworkAllowlist” or the “UidOnMeteredNetworkDenylist” (exhibit I-D9, figure 2). Depending on the respective update of “UidOnMeteredNetworkAllowlist” or the “UidOnMeteredNetworkDenylist” a respective BpfNetMap entry is created (BPF = Berkeley Packet Filter) (exhibit I-D9, figure 2). This filter either blocks or forwards packets containing the UID to the modem. The bandwidth controller therefore implements the corresponding “allow/block” filters in the firewall layer of the Android architecture. This process is shown in figure 2.

23. The *setMeteredNetworkDenylist* and *setMeteredNetworkAllowlist* are both submethods of the second main method *updateRulesForDataUsageRestrictionsULInner* ("second main method") in the Data Saver Funcionality Code.

REQUESTS OF THE PARTIES:

Infringement:

24. The Claimant requests:

I. The Defendants are ordered,

1. to refrain from offering, putting on the market, selling, using, or possessing for these purposes,

in the Federal Republic of Germany, and/or the Republic of France, and/or the Kingdom of the Netherlands,

wireless end-user devices, comprising: a processor; a wireless wide area network (WWAN) modem for communicating data for network service usage activities between the device and a WWAN when connected to a WWAN; a wireless local area network (WLAN) modem to communicate data for network service usage activities between the device and a WLAN, when connected to a WLAN; a computer-readable storage medium storing instructions which, when provided to the processor, cause the processor to determine, for a first device application, whether the application is running in a background state or in a foreground state, and control, via an application program interface, API, application access for network service usage activities provided by the WWAN modem and the WLAN modem, to, based on a first traffic control policy, selectively block and allow access by the first device application to at least one of the WWAN and the WLAN modem, wherein the access is selectively blocked based on a determination that the first device application is running in a background state, and wherein the access is selectively allowed based on a determination that the first device application is running in a foreground state;

(claim 1 of EP 3 110 069 B1)

2. to, within 30 days from the service of the decision on the merits, provide the Claimant with information, structured by each month of a calendar year, on the extent to which they have committed the acts described in Section I.1. since 16 August 2017, stating

   a) the origin and distribution channels of the products referred to in point I.1.;

   b) the delivered, received and ordered quantities, and the prices paid for the products referred to in point I.1.;

   c) the names and addresses of all third parties involved in the production and the supply of the products referred to in point I.1.;

   d) the quantity and identifying data of the products offered;

   e) the advertising carried out with respect to the products referred to in point I.1., broken down by advertising mediums, their distribution, the distribution periods and the distribution areas; including evidence of these advertising activities;

   whereby copies of the corresponding purchase documents (namely invoices, alternatively delivery notes) must be provided, whereby details requiring confidentiality outside the data subject to disclosure may be blacked out;

3. to recall the infringing products referred to in point I.1. by informing the third parties from whom the infringing products are to be recalled that the Unified Patent Court, Local Division Düsseldorf, has found that the products

infringe European Patent EP 3 110 069 B1; whereby the Defendants must give the third parties a binding undertaking to (i) reimburse their costs incurred, (ii) bear the packaging and transportation costs, as well as the customs duties and storage costs associated with the return of the products, and (iii) take back the products;

4. to permanently remove the infringing products referred to in Item I. from the distribution channels by demanding from third parties, which are commercial buyers but not end-users, with reference to the fact that the Unified Patent Court, Local Division Düsseldorf, has found that the products infringe European Patent EP 3 110 069 B1, to cancel all orders for these products, and provide the Claimant and the Court, within the aforementioned period of 30 days after service of the enforcement notice in accordance with R. 118.8 RoP and, if applicable, a certified translation, with written proof about the performance of the actions to remove.

II. The Defendants are ordered to pay a penalty to the Court,

1. in each single event of a breach of the order under Item I.1. in the amount of up to € 250.000,00;

2. for each day of violation of the orders under Item I.2. in the amount of up to € 250.000,00.

III. It is decided that the Defendants are obliged to compensate the Claimant for all damages that Claimant incurred and will incur as a result of the acts listed under Section I.1., which the Defendants committed since 16 September 2017.

IV. The Defendants are ordered to pay provisional damages to the Claimant in the amount of € 200.000,00.

V. The Defendants are ordered to bear the costs of the litigation.

VI. The judgement is directly enforceable; in the alternative (if a security for enforcement is ordered), the Claimant is authorized to provide this security in the form of a bank or savings bank guarantee, and the amount of the security shall be determined separately for the individual operative clauses of the judgment.

25. The Defendants request

I.

1. to dismiss the action;

2. to order the Claimant to pay the costs;

in the alternative, if the Court finds patent infringement,

3. to refrain from issuing a permanent injunction pursuant to Art 63 (1) UPCA and/or corrective measures pursuant to Art. 64 UPCA;

in the further alternative

4. in lieu of permanent injunctive relief, award the Claimant reasonable monetary compensation in an amount to be determined by the Court in its sole discretion;

in the further alternative

5. to suspend the permanent injunction for a reasonable period of time, at least for 6 (six) month;

in the further alternative

6. to make the enforcement of the decision dependent on the provision of security, which may also be in the form of a bank guarantee (Art. 82 (2) UPCA, R. 352.1, 354.1 RoP);

in the further alternative,

7. to allow the Defendants to avert enforcement of the judgment by providing security, which may also be in the form of a bank guarantee, without regard to any security provided by the Claimant (R. 9.1 RoP).

Counterclaim for revocation:

26. The Defendants request

1. to revoke the patent in suit, European patent 3 110 069 B1 to the extent of claim 1 and

2. to order the Claimant to pay the costs.

27. The Claimant requests

1. to reject the Counterclaim for revocation against claim 1 of European patent EP 3 110 069 B1 ("patent in suit") in its entirety,

2. as an auxiliary measure:

to reject the counterclaim for revocation against claim 1 of European patent EP 3 110 069 B1 to the extent that claim 1 extend beyond the version according to one of the auxiliary requests 1 to 26 submitted as

- Exhibit ES_CC-1 -

wherein these auxiliary requests shall be considered in numerical order. Claimant, however, explicitly reserves the right to request a different order should the course of the procedure deem this more efficient;

3. to order the Defendants to bear the costs.

28. The Defendants request,

1. to hold that

a) the auxiliary request 1 to 26 submitted by Claimant are not allowable and to reject the auxiliary requests;

b) in alternative, to hold that the patent in suit cannot be maintained as requested by Claimant in any of the auxiliary requests 1 to 26;

2. and to dismiss the application to amend the patent;

3. in the alternative: to dismiss the infringement action for reasons of non-infringement;

4. to order the Claimant to pay the costs.

29. Claimant´s requests set out in the Reply to the Statement of Defence dated 19 August 2024 ("in particular, if" concerning alleged infringement of dependent subclaims 2, 3, 4 and 8), in the Rejoinder to the Reply to the Counterclaim for Revocation dated 21 November 2024 (cf. 3 and 4) and in the Reply to the Defence to the Application to amend the patent dated 21 November 2024 (cf. 3 and 4) as well as Defendants´s requests set out in the Reply to the Defence to the Counterclaim for Revocation dated 21 October 2024 (cf. 1 and 2) and in the Rejoinder to the Reply to the Defence to the Application to amend the patent dated 23 December 2024 (cf. 1c) and 1d)) have become obsolete. The Judge-Rapporteur already dealt with them in cf II. and III. of her order issued on 11 June 2025. She rejected the leave to change claims relating to the alleged infringement of dependent subclaims 2, 3, 4 and 8 and dismissed Defendants´ additional requests in the counterclaim with respect to these subclaims. In consequence, Claimant´s conditionally filed auxiliary requests (27 to 52, exhibit ES CC-8) are also no longer part of the proceedings. Further reference is made to Court´s order issued on 11 June 2025.

30. In the same order the Judge-Rapporteur dismissed Defendants´ applications to order the Claimant and/or […] as a third party to produce evidence pursuant to R. 190.1 RoP.

POINTS AT ISSUE:

A. Standing to sue

31. Defendants argue that Claimant is not the sole person entitled to the national parts of the patent in suit. Inventors (1) and (2) have not been owners of the respective (alleged) invention since the (alleged) invention is covered by the patent assignment agreements between […], making […] at least co-owner of the claimed ideas and of the patents derived from respective patent applications.

B. Claim Construction

I. Wireless end-user device (feature 1.1)

32. Defendants state that the wording of the claim does not exclude personal computers. If a personal computer comprises the WLAN and the WWAN functionality, it is capable of communicating wirelessly.

II. Instructions, when provided to the processor, cause the processor to determine for a first device application whether the application is running in a background or foreground state (feature 1.5, 1.5.1)

33. The Defendants state that the term “device application” is contrasted by the patent in suit with the terms “operating system functions” and “other device functions”. Consequently, a “device application” must be distinguished from those other functions. They further argue that for the claimed solution the network service usage activity in question needs to be generated by the application (and not by the operation system or by other device functions).

34. Running means that the determination has to take place at a speficic moment in time, i.e. when the application is running (being executed).

III. Instructions, when provided to the processor cause the processor to control, via an application programm interface API, application access for network service usage activites provided through the WWAN modem and the WLAN modem (feature 1.5.2)

35. The Claimants argue that it is not the API just controlling the network access but controlling the access for network service usage activities (applications network capacities). The network service usage activity can involve any activity for which an application requires network access. These activities include but are not limited to network access requests for applications. In the context of controlling to selectively block and allow access by the application to the network the meaning of controlling is not limited to blocking or allowing access in response to a specific netword usage request of an application.

36. The term application program interface and the abbreviation API is a technical term familiar to the skilled person. An API is usually made up of different parts, which act as tools or services, for building a communication interface between software programs and other components of an operating system. An API is more than a mere data bus but rather should be considered a “driver software” for certain functionalities of an operating system. Despite the slight deviation in wording (programm/programming) the patent in suit uses the term API according to its common general understanding.

37. The patent in suit describes in paragraph [0145] that the programm that corresponds to the API is used to tag application layer traffic in order to allow the agent implementing respective (traffic) policies that correspond to the information the application layer traffic has been tagged with. In other words: The API within the meaning of the claim shall be used to provide information needed for policy implementation which encompasses network access control. The purpose of the tagging is to allow traffic control.

38. The skilled person will understand from paragraph [0175] that the “first traffic control policy” mentioned in feature 1.5.3 can be an instruction or command of the API mentioned in feature 1.5.2. While not explicitly stated in the claim, this may be also derived from the context of Features 1.5 and 1.5.2.

39. The processor uses an API when executing the instructions in the computer-readable medium, as a tool for controlling network access of software applications. The API is a logical (not physical) interface between different computer programs. The API acts as an assisting intermediary in the control, not the controlling element itself.

40. The term “via” in feature 1.5.2 is thus to be interpreted as meaning that the API – as an element interfacing the application level and lower layers – assists in implementing the traffic control policy e.g. by providing a traffic flow tagging or by allowing the traffic control policy to be set based on user preferences provided via a user interface. Whether this assisting also encompasses, in some cases, that the API itself performs the control is not excluded by the

claim, but also not required by it.

41. The Defendants state that the control of traffic (“application access for network service usage activities”) through at least one of the modems needs to be affected “via an application program interface, API”. The specific wording “via” demonstrates to the skilled person that the application program interface has to function as a relay, i.e. a means through which control information is forwarded from one end to the other end, between the application on the one side and the modem on the other side. This understanding is supported by different examples (e.g figure 4) showing how the term „via“ is used in the context of the invention. In every single one of these usages of “via” it is made clear that this term teaches that something must happen by using a specific item to forward information from end to the other end. According to the claim it is the API that has to perform that function of controlling (namely blocking or allowing) application access between the application (as sender – cf. below) and the modem (as receiver).

42. The term “application program interface” as used in the claim language is not described in the patent specification as such. In the description the abbreviation is used for application interface and the description shows a multifold use for different APIs (e.g. figure 3). The skilled person understands that an “Application Program Interface, API” in accordance with the claim is an interface provided to the application allowing the application to use services provided by the API on the basis of messages/commands.

43. The Defendants are not in favour of a broad understanding of the claimed API (connecting different software programs with each other). Instead, the claimed API needs to act between the application running on the device and the network elements. There is no arbitrary connecting of software but, instead, Figure 12 of the patent in suit illustrates the relationship between application, API and the rest of the system.

44. In paragraph [0145] the patent in suit describes an application interface agent which is not defined as the program that corresponds to the API. The common understanding of software agents are computer programs which are autonomous, self-dynamic and able to carry out a specific processing operation assigned to them without additional external signals or intervention. This definition is in stark contrast with an API, which just provides for standardized interface to an application and allows an application by means of routines standardized in that interface (messages, commands) to make use of services that are provided by deeper layers of an operating system. This distinction leads to an understanding that the interface providing access to a software functionality is clearly not identical with the software program to which access is provided. This is supported by figures 3 and 12 showing agents as additional soft- or hardware elements which are seperate from the API & OS Stack Interface. Agents are not the interface between application and network elements and therefore are no API in the meaning of the claim but something different. Defendants finally argue that this understanding is fully in line with the second priority document of the patent in suit introducing software agents to perform proxy service functions.

45. According to the Defendants it is the “application access for network service usage activities” which needs to be controlled. An application having generated such an activity tries to access the modems. This application access for network service usage acitivity is the object of the control in the claim.

IV. Feature group 1.5.3 controls (application access) to, based on a first traffic control policy, selectively block and allow access by the first device application to at least one of the WWAN and WLAN modems (feature group 1.5.3), wherein the access is selectively blocked based on a determination that the first device application is running in a background state (feature 1.5.3.1) and wherein the acces is selectively allowed based on a determination that the first device application is running in a foreground state (feature 1.5.3.2)

46. Claimant argues that, in the context of the patent in suit, the term "allow" is to be understood as simply describing the alternative to block. However, the patent in suit does not consider a queuing of traffic as a (temporary) blocking thereof.

47. The patent in suit does not specify the (one) foreground state and the (one) background state. There are multiple states in which the application may run, each of which may either be considered some sort of foreground state and some sort of background state.

48. Instead of foreseeing one single background state and one single foreground state, the patent in suit rather considers the terms "foreground" and "background" to designate a number of different states which have a certain fluidity, as a certain application may running in the background state at one moment in time and running a foreground state at another moment in time, even if the network service usage activity does not change as such.

49. Depending on the state of the application, the first traffic control policy to be applied to this devices application is adjusted accordingly. This also follows from sub-claim 11.

50. Feature 1.5.3 provides that that processor shall selectively block and allow access (to at least one of WWAN and WLAN network via respective modems) of a first device application *"based on"* a first traffic control policy. According to the Claimant it follows from the wording "based on" that the blocking or allowing of network access shall take a (first) traffic control policy into account. The claim wording, however, clearly does not require that the traffic control policy is the only policy or instruction that causes the processor to block or allow network access for a specific application. The same applies for sub-features 1.5.3.1 and 1.5.3.2 to the extent that the access is blocked/allowed "based on" the determination that the device application is running in a background state/foreground state. That is, the traffic control policy and the process state of the application (background/foreground state) to which the policy shall apply, simply needs to be taken into consideration by the processor when deciding to either block or allow network access for that application.

51. The Defendants argue that the claim does not mention different "sorts" of background/foreground states on the application level. Likewise sub-claim 2 specifically relates to the running in a background state to the application and not to an activity generated by the application, i.e. not to the network service usage activity.

52. Application and network service usage activity are not synonyms but address different technical aspects. Nothing else can be drawn out of pararaph [0021] of the patent in suit because it specifically refers to the device service activity behaviour generated by applications that impacts the network performance, too.

53. While the patent description does not deal with the foreground or background state of the application, the claim explicitly refers to it while differentiating the term "application" from the term "network service usage activity".

54. For the control of blocking or allowing access (feature 1.5.3), the determination that an application is running in a background or a foreground state is not simply contributing to the decision to block/allow the network access. The skilled person understands that there must be at least one use case where the outcome of blocking/allowing is solely based on the determination of background/foreground state (and not on a mix of criteria that could e.g. counteract or override any such determination of background / foreground state). The "selectively" blocking and allowing is related to the application accessing the modem, i.e. the patent in suit requires a blocking/allowing control on an application basis.

55. The Defendants further argue that the claimed wording of the selectively blocking and allowing "based on" the determination of the application running in a background/foreground state is not disclosed anywhere in the description.

56. Selectively means that for each application´s access attempt it needs to be decided whether it needs to be blocked or needs to be allowed. Sub claim 11 deals with a scenario in which the usage (application) of the first traffic control policy is changed which is precisely not the case in claim 1.

C. Infringement

57. Claimant states that the attacked embodiments infringe the patent in suit due to their Data Saver functionality.

58. The instructions of the Android operating systems stored in the memory of the attacked embodiments cause the processor to determine whether a specific application is currently running in a background state or in a foreground state. The application´s background or foreground state is also decisive when the data saver mode is "on" as network service usage requests of apps will be rejected only if it is determined that the app is running in the background state.

59. The Defendants argue that Claimant attacks in essence three different functionalities of the Android 7 (or higher) operating system, none of them leading to an infringement of the attacked embodiments.

60. The processor does not control application access to the modem for network usage activities via an API. The control of the modem access in the attacked embodiments is performed on a Kernel level rather than on an application programm interface level. There is no infringement as the processor does not determine whether a first device application is running in a background state or in a foreground state within the meaning of the patent in suit.

61. The technical function of the PROCESS STATE (variable "*procState*") is to enable the Android operating system to decide on killing a process in order to free memory space which is completely different from the claimed determination. Apart from the foreground processes, the Linux process states as such do not indicate whether an application is actually running. There is no selectively allowing of application access.

62. Besides lack of selective allowing, there is also no infringement of option #1´ because, for applications running in a foreground state the Data Saver setting on/off is never decisive and for both whitelisted and denylisted applications, the Data Saver setting on/off is never decisive. *ProcState* does not return whether the application is running, there is no determination

whether the application is running in a background state.

63. Also in option #2´ and option #3´ there is no allowing at all. There is no determination of a running status of an application and no controlling of access to the modem via an API. For option #2´, it is only decisive that the UID of an application is listed in the PENALTY Box. For Option #3´ it is only decisive that the UID of an application is listed in the HAPPY Box.

D. Validity

64. Defendants argue that the patent in suit is invalid due to added-matter, lack of novelty, inventive step and lack of entitlement.

65. With regard to the arguments put forward by the parties, reference is made to the written submissions and annexes, as well as to the recording of the oral hearing.

GROUNDS FOR THE DECISION:

66. Both, the counterclaim for revocation and the infringement action, are admissible. The counterclaim is well-founded, the infringement action being already unfounded as a consequence of the invalidity of the patent in suit.

A. International Jurisdiction

67. The Düsseldorf Local Division has international jurisdiction on the basis of Article Art. 7(2) in conjunction with Art. 71b(1) of the Brussels I recast Regulation as the attacked embodiment is (also) offered and distributed within Germany. The Court has international jurisdiction for the counterclaim for revocation on the basis of Art. 24(4) in conjunction with Article 71b(1) and 71a.2 sub a of the Brussels recast Regulation. The Düsseldorf Local Division is furthermore competent according to Art. 32(1) (a), (e), 33(1)(a), UPCA.

B. Scope of Protection

68. To answer the questions of infringement and validity, the claim has to be interpreted by the skilled person at the priority date in order to define its scope of protection.

I. Skilled person

69. The person skilled in the art has a university/engineering degree with a specialization in wireless devices and network technology.

II. Prior Art and Claim Construction

70. The patent in suit relates to the field of wireless networks. More specifically, the invention relates to device-assisted services for protecting network capacity.

71. Starting with the background section, the patent in suit refers to prior art US 2003/0028623 A1 basically showing a system that facilitates receiving content at a client from one or more servers that can potentially provide this content. The patent in suit goes on by pointing out that, with the advent of mass market digital communications applications and content distribution, many networks are overloaded with user capacity. In the wireless case although network capacity will increase the patent in suit predicts that these future capacity gains are likely less than what is required to meet growing digital networking demand.

72. The patent in suit does not formulate a specific task to be solved but rather generally refers to network capacity constraints due to increasing digital networking demand. The skilled person reading the specification takes into account the growing network capacity crunch in para. [0008] and the addressed observation that a relatively small number of users on such devices may demand a disproportionately significant amount of network capacity. Further, the patent presents an overview of the known solutions for improving network resource usage (para. [0009]; paragraphs hereinafter which do not contain any source of citation are those of the patent in suit and abbreviated as para.). These solutions traditionally rely on mobile devices with specialized designs, optimized to preserve network resources (para [0011]), but of higher complexity [para. [0013]).

73. Furthermore, the skilled person understands that the network capacity crunch can also be caused by other types of persistent or frequent traffic network interaction. According to the

patent in suit, the demand for network capacity can be reduced by controlling network service usage activities of wireless communication devices within a network (see para. [0031]).

74. Against this background, the skilled person identifies maintaining the network capacity and avoiding the capacity crunch as the technical problem underlying the patent in suit. This technical problem is allegedly solved by the device of claim 1.

75. Claim 1 can be structured by means of the following features:

1.1 A wireless end-user device (100), comprising:

1.2 a processor (115);

1.3 a wireless wide area network, WWAN, modem (1812) to communicate data for network service usage activities between the device and a WWAN, when connected to a WWAN;

1.4 a wireless local area network, WLAN, modem (1813) to communicate data for network service usage activities between the device and a WLAN, when connected to a WLAN;

1.5 a computer-readable storage medium storing instructions that, when provided to the processor (115), cause the processor (115) to

1.5.1 determine, for a first device application whether the application is running background state or in a foreground state, and

1.5.2 control, via an application program interface, API, application access for network service usage activities provided through the WWAN mo dem (1812) and the WLAN modem (1813),

1.5.3 to, based on a first traffic control policy, selectively block and allow access by the first device application to at least one of the WWAN and WLAN modems (1812, 1813),

1.5.3.1. wherein the access is selectively blocked based on a determination that the first device application is run ning in a background state, and

1.5.3.2 wherein the access is selectively allowed based on a determination that the first device application is run ning in a foreground state.

III. Basic legal framework for claim interpretation

76. The interpretation of the claims is governed by Art. 69 EPC and the Protocol on the Interpretation of Art. 69 EPC in conjunction with Art. 24(1) c) UPCA. The same approach to claim construction is to be used when assessing infringement and validity; thus, Art. 69 EPC must be the governing principle in claim interpretation also in the context of validity. The understanding of a claim by the skilled person must be consistent for all purposes of the evaluation of infringement and validity (UPC_CoA_335/2023, Order of 26 February 2024, Headnote 2 –

NanoString v 10x Genomics).

77. Art. 69(1) EPC stipulates that the description shall be used to interpret the claims. The Protocol on the Interpretation of Art. 69 EPC, in its Art. 1, sets the general principles for claim interpretation. One of these principles of the Protocol is that Art. 69 EPC should not be taken to mean that the claims serve only as a guideline and that the actual protection conferred may extend to what, from a consideration of the description and drawings by a person skilled in the art, the patent proprietor has contemplated. The Protocol, in using the term "extend," clearly intends to prevent a claim interpretation which extends the subject-matter beyond what is actually claimed, i.e. exceeds the boundaries of the claim. The underlying legal principle is legal certainty.

78. Art. 69 EPC and its Protocol require that the terms used in the claims must govern claim construction, on their own or in their claimed combination. They are not just the "starting point" for claim construction but the authoritative basis for determining the scope of protection. The description and the drawings are nevertheless always to be considered, even with seemingly clear claims; thus, a patent may be used as its "own lexicon" (UPC_CoA_335/2023, Order of 26 February 2024, Headnote 2 – NanoString v 10x Genomics; UPC_CFI_14/2024 (CD Munich), Decision of 16 July 2024, Headnote 1 – Regeneron v Amgen).

79. The features of a claim have to be read in combination, as they must always be interpreted in the light of the claims as a whole (UPC_CoA_1/2024, Order of 13 May 2024, mn 29 – VusionGroup v Hanshow). Nothing else must apply to a combination of features resulting from combining a dependent claim with the features of the claims it depends from.

80. Art. 69 EPC and its Protocol therefore establish a primacy of the claims.

IV. Claim interpretation

81. In respect of the dispute of the parties some of the features require further interpretation.

1. Feature 1.1 - "wireless end-user device"

82. The claimed wireless end-user device comprises a WWAN modem (feature 1.3) and a WLAN modem (feature 1.4). Such a device is therefore able to connect to a WLAN such as a WiFi network and to a cellular telecommunication network such as 3G, LTE, 4G, 5G. Hence, smartphones and tablets can generally be regarded as wireless end-user devices whereas personal computers qualify this term if they are able to connect to both types of networks.

2. Feature group 1.5. – structure

83. Feature group 1.5 including features 1.5.1 to 1.5.3 and 1.5.3.1 and 1.5.3.2 determines certain operations the processor is able to perform when it is provided with instructions stored in the computer-readable storage of the claimed device.

84. In simple terms, the processor is caused by instructions to

a) determine a certain state of the application (features 1.5.1, 1.5.3.1, 1.5.3.2)

b) control via API the access for network service usage activities to selectively block or allow access depending on the determined state of the application (features 1.5.2 and 1.5.3).

85. After determination of the foreground or background state, the content of the control consists of selectively allowing the access or selectively blocking the access for network service usage activities.

a) Network service usage activities

86. The person skilled in the art construes the term “network service usage activity” broadly as any activity making use of the network resources (WWAN or the WLAN) according to feature 1.5.2.

87. According to the wording of the claim, the skilled person will distinguish between a (first device) application and the network service usage activity. The skilled person will acknowledge that, unless otherwise specified in the patent in question, different technical terms in a claim usually refer to different technical concepts. The claim refers to application access for network service usage activities. The application access for network activities is the object of the control.

88. The wording of the claim leaves open by which means the network service usage activities are generated. Moreover, para. [0036] states that in some embodiments a network service usage activity is any activity by the device that includes wireless network communication. In some embodiments, an application, an operating system (OS), and/or other device function generates a respectively one or more network service usage activities. Para. [0021] is not relevant at this point because it relates to device service activity behavior rather than network service usage activity.

89. A broad understanding is also confirmed by the inconsistent use of the term in the description. Para. [0036] names many different examples of network service activities. In some examples, it seems to encompass applications without being limited to them (para. [0210], [0236]). In other examples, it seems to relate to various types of connections or other network services (para. [0036]). As examples of such service activities (performed by the processor of the device), the patent in suit mentions, inter alia, the updating of software or (device) applications, cloud synchronisation, downloads or also text/voice/video/chat activities, or network access in the background, such as updates of individual device applications (paras. [0022] and [0049]).

b) running in a background state/running in a foreground state

90. The skilled person understands an “application running in a background state” (or more commonly “running in the background”) as an application which, at a given point of time, does not directly interact with the user and does not provide any benefit to the user. Conversely, an “application running in a foreground state” is an application which either directly interacts with the user or provides a benefit to the user.

91. The technical function of the determination of the two states is to prepare the allowing/blocking decision by the processor, which depends on the result of this determination. Controlling the application access for network service usage activities serves the purpose of reducing traffic not benefiting to the user at a given time and avoiding the network capacity crunch.

92. Para. [0021] and sub-claim 2 outline what the patent in suit means by running in a background. It states that, when a user is not directly interacting with or benefiting for this type of application behaviour (e.g. video streaming, software update, […], the application can be

running in the background).

93. The claim requires that the application “is running”. In para. [0283], the patent in suit uses the term “running” in an example: “The application can be refered to as “running” on the device or as being “executed” by the device in accordance with known uses of those terms.” Therefore, at the moment foreground/background state is determined, the application is running. The moment of the determination is a specific moment in time.

94. Contrary to Claimant’s view, the term does not designate a number of different states which have a certain fluidity. Although a given application may run in the background state at one moment in time and run in a foreground state at another moment in time, even if the network service usage activity does not change as such, that does not lead to a fluidity of states within feature group 1.5.1. The claim relates to a specific situation: at a moment in time one state of the running application is determined – either foreground or background. The claim does not exclude that this determination and control is repeated several times during the use of the device and that the state changes from one moment to another. However, in such instance, all the steps of feature group 1.5 will be repeated.

c) “control, via an application program interface, API”

95. An application program interface (or rather an application programming interface, API) is basically an interface which is made available by a software system to applications for connection to the latter. The API offers to applications the possibility of using (calling) subroutines of the interface without knowing how the system works. In the claim the processor can control application access to so-called “network service usage activities” via the interface, *i.e.* by calling subroutines of the interface. Although there is no definition in the description of the API, this understanding seems is in line with relevant passages of the description and the common knowledge of the skilled person.

96. The control via the API is not limited to a control performed only via the API itself, but possibly includes an assisting intermediary in the control.

97. The scope of this expression is broad, demanding nothing more than the control via an API without more detailed information about specific functions thereof.

98. First, the Claimant’s reference to paras. [0023] and [0026] is not relevant, as these paragraphs only refer in general to degrading network capacity and to some embodiments for protecting network capacity including controlling network service usage activities at the source of the device. An API is not mentioned there.

99. However, para. [0201] of the description gives a more specific definition of a so-called device service access API. It provides an interface for applications, OS functions and/other service usage activities to a network access connection for providing differential network access for protecting network capacity. The more general understanding (rather than a mere data bus) is also supported by para. [0145] stating that in some embodiments an application interface agent is used to literally tag or virtually tag application layer traffic so that the policy implementing agents has the necessary information to implement selected traffic shaping solutions. An agent cannot be equated with an API, as it is a software unit characterized by its capability to perform an assigned (or delegated) task in an autonomous way without requiring any further signals or an external control intervention while possibly communicating with

other agents during the process. However, the API is an interface made available by a software system for applications requesting an access thereto without disclosing how the system works. Using additional agents as assisting intermediary is not excluded by the broad wording of the claim “to control, via an […] API”.

100. In addition, para. [0175] supports the understanding that the control via the API is not limited to a control performed by the API itself, but also includes an assisting intermediary. This paragraph depicts embodiments where Device Assisted Service (DAS) for protecting network capacity includes providing a network access API, e.g. such an API can provide network busy state informations and/or other criteria/measures and/or provide a mechanism for allowing, denying, delaying, and/or otherwise controlling network access.

101. In contrast, Defendants argument how the term “via” is used in different embodiments at different description passages does not convince the Court as the word “via” is used in totally different contexts in these examples. Also figures 12 and 3 do not contradict the skilled person´s interpretation outlined above. Both figures show the mentioned agents. Being only examples of the claimed invention, they show the additional agents and their connection to a data bus. These embodiments as such do not limit the scope of a control via an API.

d) to selectively block and allow access

102. The skilled person understands that allowing access is the opposite of blocking access. The processor does not interfere with a network service usage request when it is determined that the application is running in a foreground state.

103. The claim does not require any sort of “activity” or “positive authorization”. The description mentions as a traffic control policy using DAS techniques the alternative allowing/blocking (para [0242]). Defendants´ argumentation that a processor does not “let something” happen is beside the point. The decision of the processor of “not blocking” simply is “allowing”. How this is implemented in the code may be another question, but the patent in suit does not deal with this configuration. Selectively blocking and allowing in the context of feature group 1.5.3 means that the device makes decisions about each application access to the network based on the determination of the background/foreground state of the application in features 1.5.3.1 und 1.5.3.2.

C. Counterclaim for revocation

104. The counterclaim is well-founded because the invilidaty attack based on added matter is successful.

I. Added matter Art. 138 (1) c), Art. 65 (2) UPCA

1. General principles

105. The Defendants argue that the subject-matter of claim 1 extends beyond the content of the earlier patent application as filed, Art 76(1) EPC. The criterion to determine whether a divisional application extends beyond the content of the parent application (exhibit R-Sp2; WO 2011/149532 A1, hereinafter SP2) is the same as the one applied to determine whether an application contains added subject-matter with respect to the application as originally filed, Art. 123(2) EPC.

106. In such a case, the Court must first ascertain what the skilled person would derive directly

and unambiguously using his common general knowledge and seen objectively and at the date of filing, from the whole of the application as filed, whereby implicitly disclosed subject-matter, i.e. matter that is a clear and unambiguous consequence of what is explicitly mentioned, shall also be considered as part of its content (see CoA, Decision of 14 February 2025, mn. 52, UPC_CoA_382/2024 – Abbott Diabetes Care v. Sibio Technology).

107. However, when the Court has to decide on the merits, as it is case in the present instance, the standard to be used for assessing the presence of added subject-matter is the criterion of "beyond (reasonable) doubt" (LD Düsseldorf, Decision of 28 January 2025, headnote 4, UPC_CFI_355/2023 – Fuji v. Kodak).

2. Case at hand

a) The Defendants argue that features 1.5.1 and 1.5.3.1 (resp. feature 1.5.3.2) are not disclosed in the earlier application as originally filed because, according to this application, the processor determines whether a network service usage activity is running in the background (resp. foreground), instead of whether a (first) device application is running in the background (resp. foreground), as claimed. The Court agrees with this view and finds that the main request contains added matter by applying the outlined standard above.

(1) Claimant´s arguments

108. The Claimant refutes this argument by referring to figure 27 and corresponding passage of the description, para. [00311] SP2, stating that the figure "depicts a diagram of an example of a system 2700 for application-specific differential network access control. […] The system 2700 is intended to represent a specific implementation of techniques described previously in this paper for illustrative purposes. The techniques may be applicable to an applicable known or convenient (wired or wireless) device for which there is a motivation to control network service usage." In the specific embodiment of figure 27, the application discussed in relation to para. [00311] SP2 corresponds to an application implemented on a device (para [00312] SP2). It is described that the application-specific differential network access control may be based on a classification of the traffic caused by the application (para. [00314] SP2): "[…] The network service usage classification engine 2708 can categorize the traffic stored in the application behavior datastore 2706 based on, e.g., network type, time of day, connection cost, whether home or roaming, network busy state, QoS, and whether the particular service usage activity is in the foreground of user interaction or in the background of user interaction, or other characteristics that are obtained from network service usage analysis or through other means. […]". One of the alternatives mentioned in para. [00314], SP2 is the classification of a particular service usage activity related to the application in the foreground or the background state. The particular service usage activity mentioned is to be considered as being appreciable for an application. When a network service usage activity is determined to be in the foreground, this would mean that the application that is causing said network service usage activity *is running in the foreground state*. Conversely, when the network service usage activity is determined to be in the background, this means that the application causing said network service usage activity *is running in the background state*. Therefore, Claimant argues that, in accordance with the example of figure 27, an application-specific access control is performed, based, inter alia, on the determination, *for a first device application,* whether it is running in a foreground or a background state.

(2) Court´s finding

109. This refutation does not convince the Court for the following reasons:

110. The fact that figure 27 depicts a system for application-specific differential network access control does not mean that the application is categorized as running in the background or the foreground. Rather, the network service usage analysis engine (2704) and the network service usage classification engine (2708) analyzes the traffic sent by the application and categorizes the traffic upon various criteria, one of which being that a particular network service usage activity is in the foreground or the background of user interaction (para. [00314] SP2). For doing so, the system uses classification rules (ibid.) including a service list of network service usage activities running in the background and in the foreground. Where a plurality of network service usage activities are involved in running wireless end-user device application, some of them running in the background and some in the foreground, SP2 does not disclose how such a device application would be classified. In other words, there is no disclosure of a determination for a device application whether it is running in a background state or in a foreground state.

110. Claimant´s argument that network service usage activities in the example of figure 27 are “considered” at the application level is inaccurate since the application behavior datastore, 2706, storing all or part of the traffic of the application for subsequent classification in 2708, contains data structures at different levels of the OSI stack. Once the network service usage activities have been classified, they are prioritized (figure 27, 2710) and the (network service consuming) application traffic is queued by differential network access control engine 2714 in cache 2716. Such a cache would be devoid of purpose if the access would be selectively blocked/allowed. On the contrary, the traffic control policy implemented in figure 27 is based on throttling, i.e. traffic classified as having a low priority is queued vs. traffic of higher priority.

(3) Claimant´s new line of arguments in the oral hearing

111. At the oral hearing, the Claimant stated for the first time that figure 27 is only an example but does not show the general concept the claim is based on. For deriving this general concept, the skilled person would rather take into account paras. [0049] and [0065] SP2. The very last sentence of para. [0049] SP2 shows the problem underlying the claimed invention, namely that, even when the user is not directly interacting with or benefiting “from this type of application” (i.e. an application maintaining persistent network communication), the application can be running in the background and continuing to consume potentially significant network resources. In such a case, the patent in suit would teach to perform differential network access control. The differential network access control would be reflected in the claim by the terms “block and allow”. A “block and allow” network access control is one example of the differential network control policies listed in para. [0065] SP2 as implementation of a network service usage activity policy. Such a policy can block/allow network access and nothing else. In its last sentence, para. [00267] SP2 refers to some embodiments in which a network service usage activity is determined to be an active application or process (e.g., based on a user interaction with the device and/or network service usage activity, such as a pop-up and/or other criteria/measures).

112. In line with the case law established in Tridonic./.CUPOWER (LD Düsseldorf, Decision of 7 March 2025, UPC_CFI_459/2023), Claimant´s new line of arguments has to be rejected pursuant to R. 9.2 RoP. As the issue has been raised from the outset and the new argument is

based on completely different passages of a lengthy document, neither the Court nor the other party may be forced to deal with it from scratch. Deciding otherwise would undermine the concept of front-loaded procedure established by the Rules of Procedure. In this particular case, the issue of added-matter and the disclosure of an application running in the background have been disputed from the very beginning and SP2 comprises over 200 pages. Deriving the disclosure of a feature in dispute from three parts of SP2 never mentioned before in the context of the main request of claim 1 and putting forward a new argument of a general concept the claim would be based on could easily have been done in accordance with the time limits set by the Rules of Procedure.

113. Apart from that, the argument is also not convincing on the merits. The patent in suit does not claim the general concept of a network service usage activity policy but the application access for network service usage activities based on a first traffic control policy by determining whether the application is running in a background/foreground state. There is no reason why the skilled person would derive the disclosure of an application as a special network service usage activity, and the determination of their running in the background resp. foreground, out of the combination of the three different passages, absent any further explanation to understand it that way. In particular, the reference in para. [00267] SP2 sentence fails to bridge the gap between an application and a network service usage activity. Claimant´s approach seems to be cherry-picking of different features which are not unambiguously and directly disclosed together. The disclosure of a network access control based on a classification of the network usage activity is a "red thread" throughout SP2 (from its description to claim 1), and the umbrella term "application" is not consistently used. Therefore, claim 1 contains added-matter in this respect.

b) The Court also finds that there is no API blocking access (features 1.5.2, 1.5.3) disclosed based on the determination that the application is running in the background.

114. Contrary to the Claimant's argumentation, the combination of para. [00204] SP2 with para. [00311] SP2, in relation to figure 27 fails to directly and unambiguously disclose a "network access API" selectively blocking (resp. allowing) network access for an application, depending on whether it is running in the background (resp. the foreground). In para. [0204] SP2, so-called DAS (*Device Assisted Services*) are said to provide "a network access API or an emulated or virtual network API which can provide network busy state information and/other criteria for allowing, denying, delaying and/or otherwise controlling network access*"*. The loose reference in para. [00311] SP2 to "specific implementation techniques described previously in this paper for illustrative purposes" is improper to connect with para. [00204] SP2, all the more since the system of Fig. 27 implements a policy of controlling network access based on queueing traffic in cache 2716, using a prioritization of network service usage activities by the differential access control engine, 2710. This differential access control engine can ***restrict*** network access of a particular (network) service usage activity when this activity is in the background (para. [00319] SP2). Restriction of access to the network cannot be equated to blocking but rather relates to throttling or delaying the traffic based on the prioritization performed in 2710. This interpretation is also in line with the list of network service usage activities in para. [0065] SP2, and the statement which the Claimants made themselves in context of claim construction. SP2 only discloses the restriction of a network access but not a blocking.

115. At the oral hearing, the Claimant referred specifically to paras. [00316], [00317] and [00321] SP2 in the context of figure 27 for the first time and stated *inter alia* that blocking access to the network for an application is also disclosed there. Even if the Court would consider this

argument as not constituting a new line of argument, the Court is not convinced about the disclosure of the blocked access of the application. The Claimant referred to the control policy which can prohibit the use of network and understands prohibit as blocking. According to the Claimant, the blocking is shown in para. [00321] SP2, where the device 2700 blocks chatter for an application running in the background because the application traffic prioritization engine 2710 determines that the chatter has zero priority. However, the skilled person reads the next sentence in conjunction and understands that even though, the user can be sent a notification by the application traffic override engine 2718 that their control policy prohibits the application from consuming network resources. The user can then opt to deviate from the control policy and the traffic can eventually be sent. Importantly, the skilled person does not understand that the application access to the network is blocked here because it is running in the background but rather because the chatter (report of device or user behaviour) has zero priority.

3. Auxiliary requests

116. The question whether the number (26) of the still pending auxiliary requests is reasonable in the view of the circumstances of the case can be left open. As none of the auxiliary requests 1-26 cure the objection of added subject-matter raised against the main request, theyare not successful.

II. Lack of entitlement, Art. 138 (1)(e) EPC, Art. 65 (2) UPCA

117. It is questionable whether this revocation ground is inadmissible in the case at hand, because the Defendant as a third party who is not the potential co-owner brought it forward in the counterclaim for revocation.

118. In favour of this result speaks that there is no reason of legal protection why any counterclaimant could launch this attack resulting in invalidity of the patent with effect against everyone. Theoretically, it would be then sufficient for a counterclaimant to revoke a patent by showing that the proprietor has no sole ownership. In view of such a finding, nothing has been said about the invention as such. In contrast, it does make sense in a case where the co-owner is defendant of an infringement action and raises this objection in a counterclaim, because in this relationship the co-ownership leads to a legitimate use of the patent.

119. However, the Court can leave the question open. The Claimant is entitled as the strong presumption of the register is not rebutted.

120. Claimant is the registered proprietor of the patent in suit in all national patent registers of the Contracting Member States it seeks an injunction for (see Exhibits ES 2-4). So the presumption of Rule 8.5.c) RoP applies. The Defendants have not rebutted this presumption as such by their presentation of the alleged co-ownership […]. Even if the Court were to assume that […] would automatically have been co-owner of the patent in suit ([…]), this co-ownership could only be asserted whithin the limitation period of two years respectively five years from the date of the mention of the grand of the European patent (Art. II, § 5, Art. 78 (1), (7) Patent Act; Art. L. 611-8 French Law). After this period, legal certainty based on the register shall prevail according to the law. The grant of the patent was mentioned on 16 August 2017. So, at least before September 2022, […] may have claimed for vindication. That did not happen. The period does not start if the patent owner was in bad faith by the time the patent was granted. Defendants did not present sufficient facts that Claimant was in bad faith about its sole ownership in summer of 2017.

III. Other validity attacks

121. The Court can leave open whether the other validity attacks are successful because they are not decisive for the case.

D. Infringement action

122. Considering the Court´s findings outlined above, the infringement action is without legal basis as the patent in suit is invalid and will be revoked with the extend to claim 1 of which the infringement has been claimed.

E. Claimant´s obsolete request for security for costs, R. 158 RoP

123. The Claimant elaborates once on a request for security for costs in their statement of claim but the request has not been made in the intended workflow in the CMS. The Claimant did not apply for it in the requests made in the oral hearing, so that the Court considers the request to have been withdrawn.

F. Decision on costs and ceiling

124. Pursuant to Art. 69(1) UPCA in conjunction with R. 118.5 RoP, a decision on costs had to be made. Since the Claimant has been unsuccessful in its infringement action and the counterclaim for revocation, it must bear the costs.

125. Pursuant to Art. 69(1) UPCA, the costs are to be borne up to a maximum amount determined in accordance with the Rules of Procedure. With a value in dispute of € 6,000,000.00 (claim and counterclaim), the table adopted by the Administrative Committee on April 24, 2023, on the basis of R. 152.2 RoP, which neither party has objected to in the oral hearing, the maximum limit for reimbursable costs of up is determined at € 600,000.00.

DECISION:

I. The infringement action is dismissed.

II. The European patent 3 110 069 B1 (patent in suit) is revoked to the extent of claim 1.

III. The costs of the infringement action and the costs of the counterclaim shall be borne by the Claimant.

IV. The value in dispute for the infringement action and the counterclaim is set at € 3,000,000.00 in each case.

V. The ceiling of recoverable representation costs is set at a total of € 600,000.00 for the infringement action and the counterclaim for revocation.

DETAILS OF THE DECISION:

Main proceedings ACT_3932/2023 and CC_35641/2024

UPC-Number: UPC_CFI_26/2024

Subject of the Proceedings: Patent infringement action and counterclaim for revocation

Düsseldorf on 30 July 2025
NAMES AND SIGNATURES

Presiding Judge Thomas	Ronny Thomas Digital unterschrieben von Ronny Thomas Datum: 2025.07.29 17:48:36 +02'00'
Legally qualified Judge Dr Thom	Anna Bérénice Dr. THOM Digital unterschrieben von Anna Bérénice Dr. THOM Datum: 2025.07.29 14:12:30 +02'00'
Legally qualified Agergaard	Peter Juul Agergaard Digitalt signeret af Peter Juul Agergaard Dato: 2025.07.29 15:18:40 +02'00'
Techniqually qualified Judge Augarde	Eric, Philippe, Gilles, Thierry Augarde Signature numérique de Eric, Philippe, Gilles, Thierry Augarde Date : 2025.07.29 15:42:13 +02'00'
For the sub-registrar	HEIKE BETTINA ELVIRA Strysio Digital unterschrieben von HEIKE BETTINA ELVIRA Strysio Datum: 2025.07.29 15:53:12 +02'00'

INFORMATION ON APPEAL:

An appeal against this decision may be brought before the Court of Appeal by any party whose claims have been unsuccessful, in whole or in part, within two months of service of the decision (Art. 73(1) UPCA, R. 220.1 (a) RoP, 224.1 (a) RoP).

INFORMATION ON ENFORCEMENT (Art. 82 UPCA, Art. 37(2) UPCS, R. 118.8, 158.2, 354, 355.4 RoP):

An authentic copy of the enforceable order will be issued by the Deputy-Registrar upon request of the enforcing party, R. 69 RegR.

INSTRUCTION TO THE REGISTRY:

A certified copy of the decision shall be sent to the European Patent Office and the respective national patent authorities as soon as the decision on the revocation action has become legally binding.

This decision was read in open court on 30 July 2025.

Presiding Judge Thomas

Ronny Thomas

Digital unterschrieben von Ronny Thomas
Datum: 2025.07.30 09:05:20 +02'00'