3GPP TSG-SA WG1 Meeting #100

Toulouse, France, 14 Nov – 18 Nov 2022

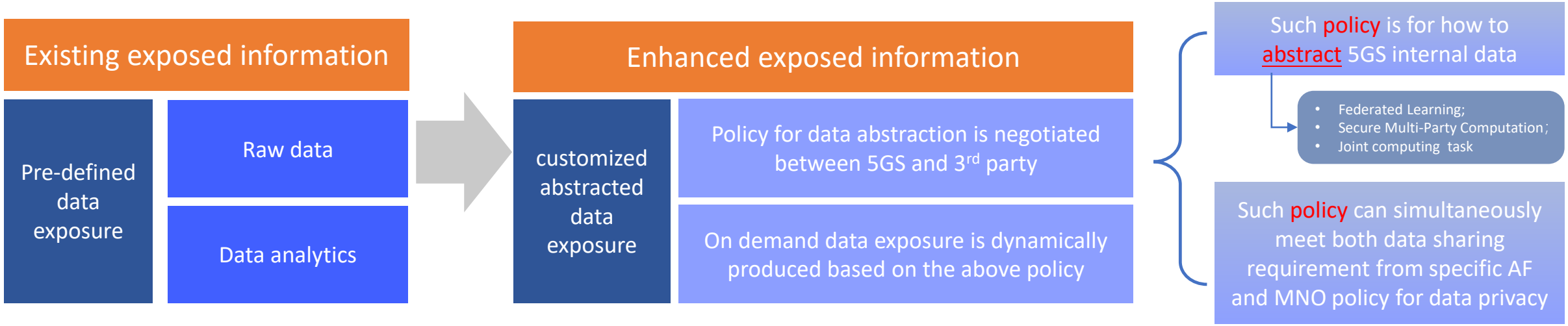
S1-223076

# Discussion on enhanced network exposure capability

vivo

# Motivation

- The core value of data lies in connection and sharing. However, there are leakage risks and security risks of confidential data and personal privacy in the circulation process, which aggravate the concerns of MNO and 3rd parties on the data circulation. Thus, existing data sharing via network capability exposure is limited subject to the operation policy, business model and other aspects of MNO and 3rd party.
- Privacy computing can help the data flow to establish an orderly and controllable sharing mechanism, and promote the vigorous development of data elements market. Inspired by the research and application progress of privacy computing, the 3GPP exposure capability can be further enhanced by supporting the customized abstracted data sharing based on the negotiated policy between MNO and 3rd party.




- With such exposure enhancement, the various data sharing requirements from 3rd parities can be fulfilled subject to MNO policy. Therefore, 3rd party and operator could achieve a win-win situation:
  - 3rd party could deliver high-end, smarter and more convenient services to ends users with low cost;
  - MNO could deliver more added-value services to 3rd parties;
  - MNO can operate networks more efficiently and deliver better communication service to end users

# Use case 1 for Tele-operated Autonomous Driving(2)

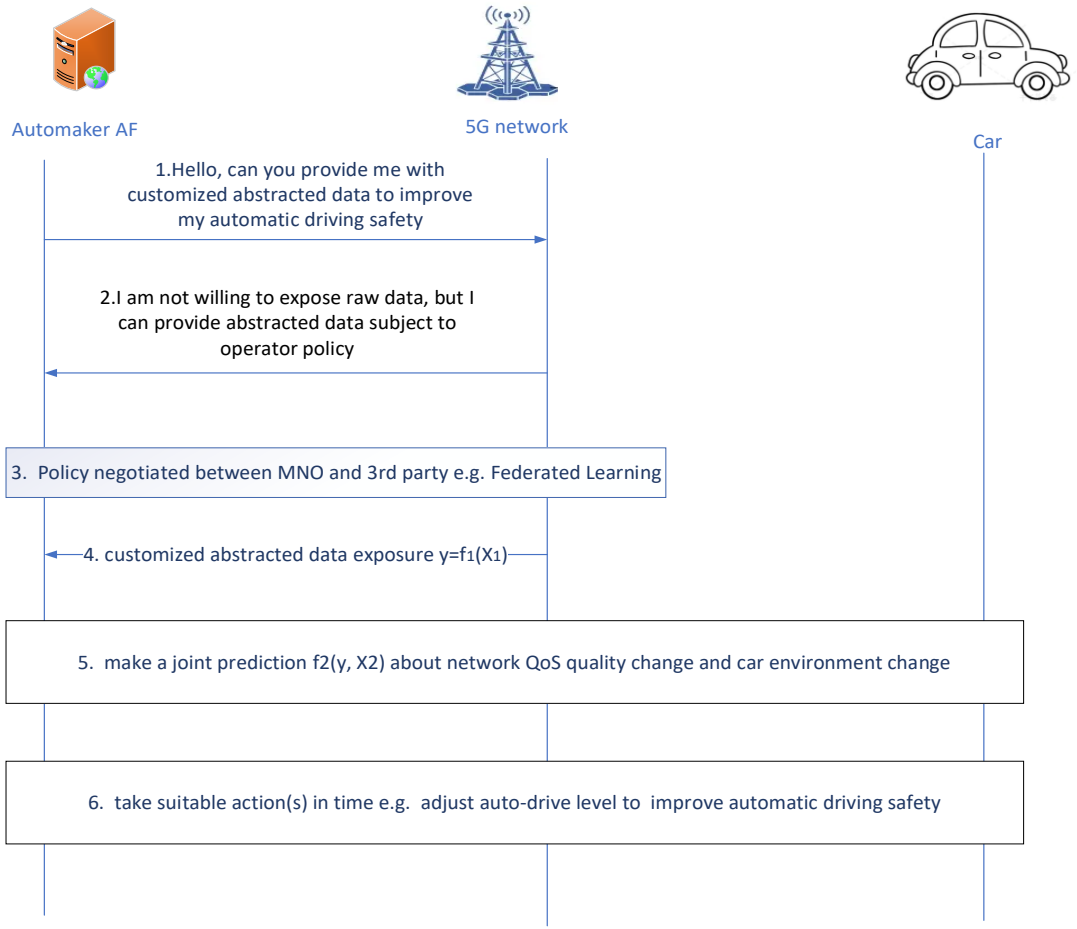
- In step 3, the policy negotiated between MNO and AF:
  - is on how to make a joint prediction:
  - contains how(i.e., y=$f_1$(x)) the MNO abstract the internal information(X1);

*Note: the policy can simultaneously meet both data sharing requirement from specific AF and MNO policy for data privacy*

- In step 4, the MNO dynamically derives the customized abstracted data y= $f_1$(X1) exposed to automaker AF

- In step 5, the automaker AF make a joint prediction $f_2$(y, X2) about network QoS quality change and car environment change.

Note: $f_2$() is AF specific algorithm, and it is out of 3GPP scope



# Use case 3 for Joint optimization by 5GS and 3rd party AS

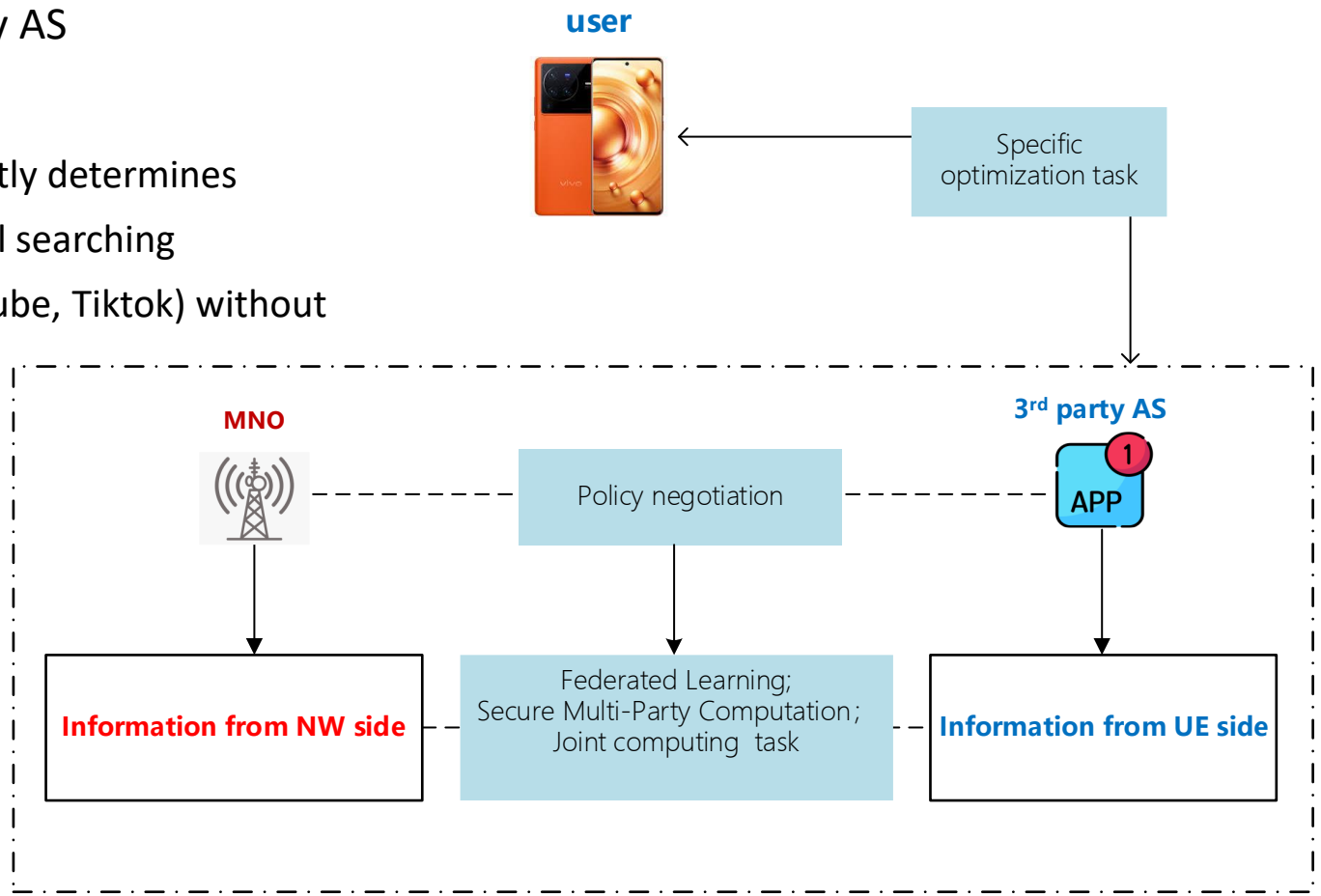
## The optimization goal:

a future value that can be used to improve user communication service experience is derived:

- by jointly computation task; and
- based on data sharing between 5GS and 3rd party AS

## Example for joint optimization :

- For areas with limited 5G coverage, the two parties jointly determines
  - strategy for inter-RAT, inter-frequency mobility cell searching
  - strategy for video streams buffering (Netflix, YouTube, Tiktok) without interruption
- Info from 3rd party side(that collected data from UE):
  - RSRP measurement results
  - Frequency/cell ID(s) of the measured cell
- Info from network side:
  - Deployment/coverage data from the network side



# Proposal

With proper abstraction of critical information exposed, the third party and the operator would have more willingness to share data between each other and provide better user service experience.

It is proposed to:

- approve the mini WID and update SA1 specification to support network exposure capability enhancement：
  - Based on operator policy, the 5G system shall provide means to negotiate with a trusted third-party the policy for customized abstraction data exposure.
  - Based on operator policy, the 5G system shall enhance data exposure (framework)capability to expose customized abstracted data to 3rd party without data privacy exposure.
  - Based on operator policy, the 5G system shall be able to provide suitable and secure means to enable an authorized third-party to provide the 3GPP network with the data analytics expected from the 3GPP network.
  - Based on operator policy, the 5G system shall be able to provide secure means for providing data analytics to authorized third-party.

  *Note: the data analytics exposure is supported in SA2 since R16 however the requirement is missing from SA1(highlighted in yellow) and it is open to whether capture it in SA1 in R19.*

vivo

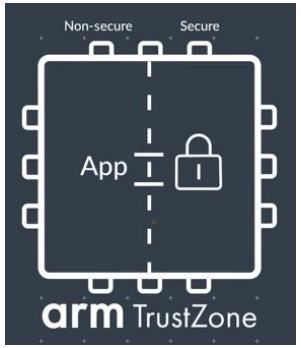
# THANK YOU.

www.vivo.com

# Background(1)

With the rapid development of 5G, internet of things, cloud computing, industrial Internet and other technologies, the amount of data has entered the stage of explosive growth. Massive data releases huge social and economic value and needs to be securely stored and shared. In recent years, there is a general consensus in the industry and academia that privacy computing will become an effective tool to balance data value mining and data privacy protection.[1]

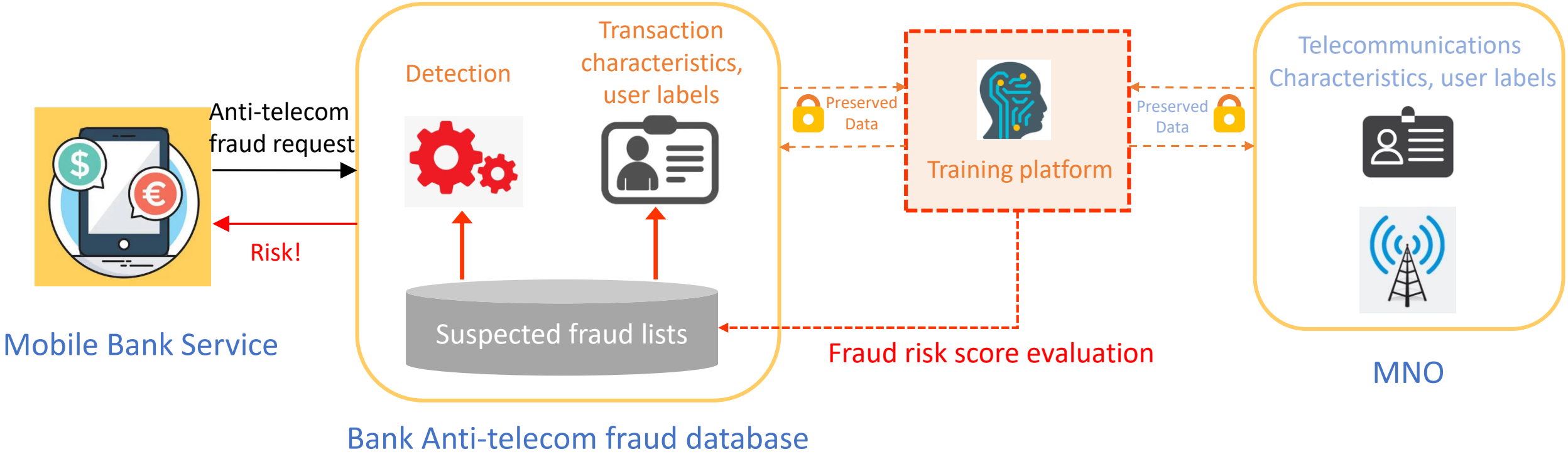
Multiple companies and researchers join this track. Google has been developing the Private Join and Compute[2] based on Secure Multiparty Computation (MPC) to enable joint analysis of data coming from multiple sources while maintaining the privacy of each input source. Meta develops Crypten[3] to enhance machine learning under privacy computing. Besides, Ant Group contributes to Secret Flow[4] for privacy-preserving data analysis and machine learning. ARM introduces TrustZone technology[5] to build a secure zone by hardware separating an operating system running raw data on the CPU efficiently and securely, along with Intel developing SGX[6] to enhance the Trusted Execution Environment study to promote the data privacy protection level. Moreover, privacy-preserving is also used in mobile advertisements[7] and vehicle Ad Hoc network[8] studies.



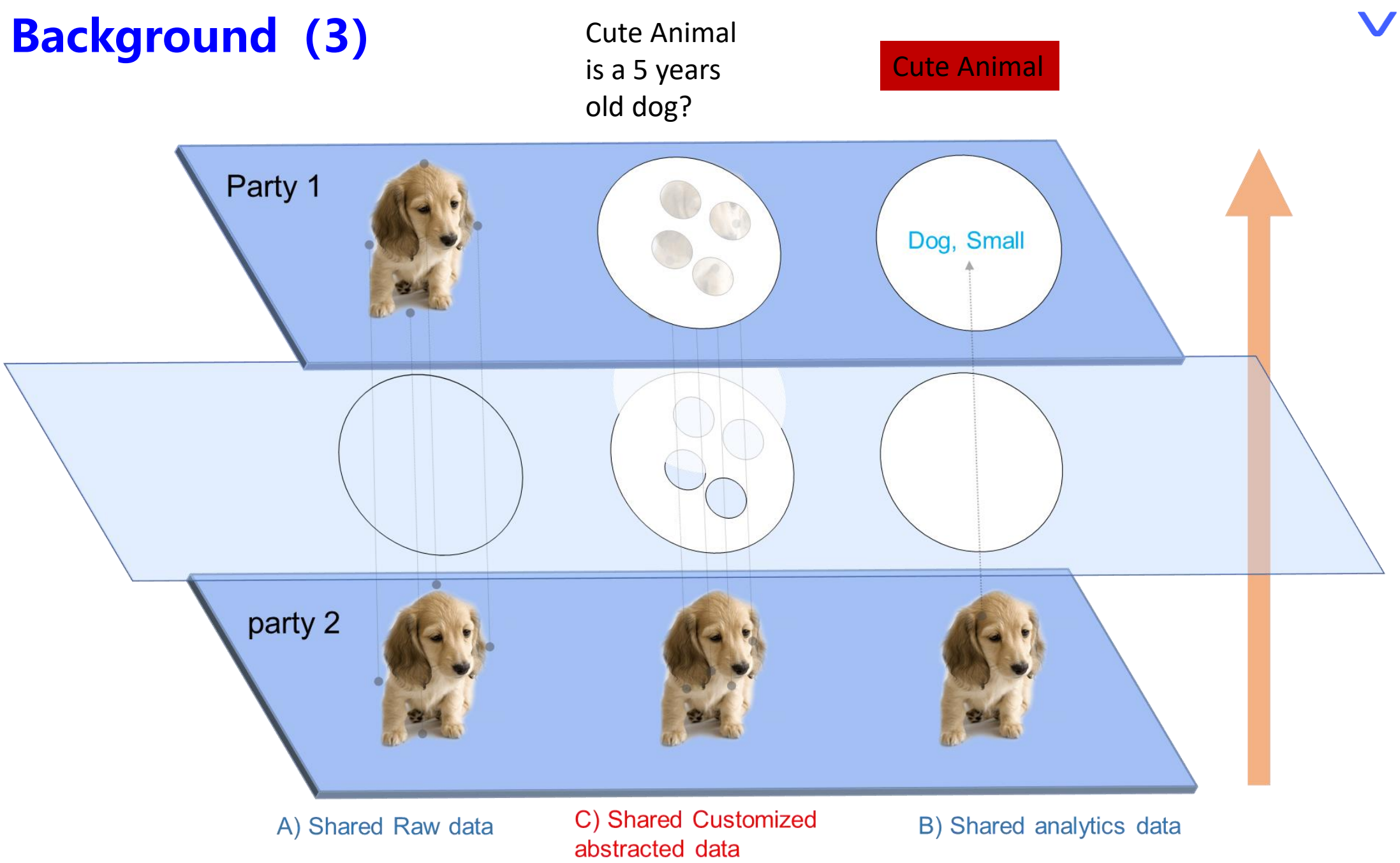
# Background(2)

## Example: Anti-telecom fraud scenario

In the practice of financial risk prevention, the privacy computing technology is utilized in order to improve the accuracy of anti-telecom fraud. On the premise of not disclosing user private information, the association relationship of interactive accounts and telecommunication accounts is conducted for secure handover, which helps banks detect normal transactions, identify abnormal transactions, improve the level of anti-telecom fraud and protect customer funds safety. [9] provides analysis for Fraud Detection in Mobile Payments Utilizing Process Behavior.



# Background (3)



# Background(4)

- Existing network capability exposure is defined since R15 which are composed of 3 parts:

  1) Existing network data defined in TS 23.502

| Functionality | 3GPP←→outside AF | Description |
|---|---|---|
| Monitoring capability | → | For monitoring of specific event for UE in 5G System and making such monitoring events information available for external exposure via the NEF |
| Provisioning capability | ← | For allowing external party to provision of information which can be used for the UE in 5G System |
| Policy/Charging capability | ← | For handling access and mobility management, QoS and charging policies for the UE based on the request from external party |
| Analytics reporting capability | → | For allowing an external party to fetch or subscribe/unsubscribe to analytics information generated by 5G System |

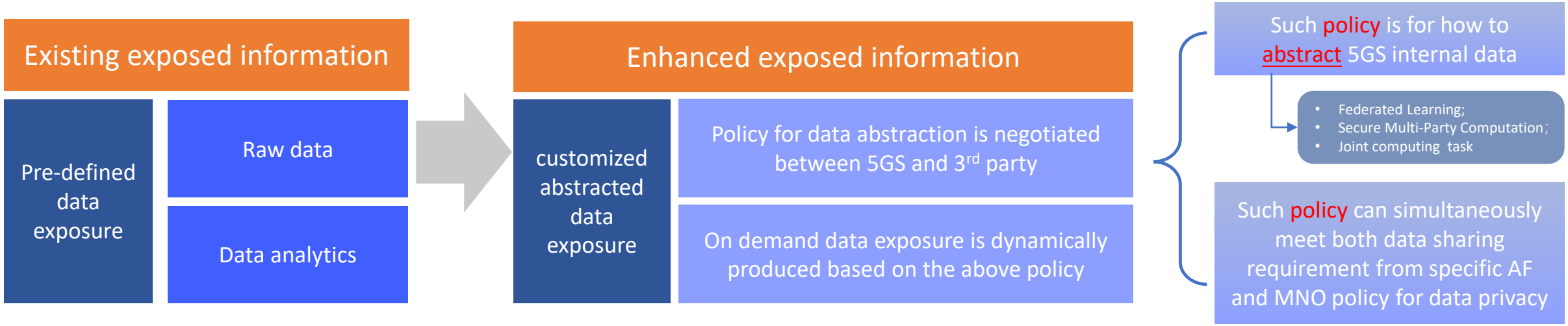
2) Existing network analytics defined TS 23.888
   - User Data Congestion Analytics in clause 6.8
   - QoS Sustainability Analytics in clause 6.9
   - UE mobility analytics in clause 6.7.2
   - etc.

3) Existing management capability defined in e.g. TS 28.533/TS28.552
   - Management service provided by management function

Though 3rd AF has strong requirement, network data exposure so far is limited subject to operator data policy

# Motivation

- The core value of data lies in connection and sharing. However, there are leakage risks and security risks of confidential data and personal privacy in the circulation process, which aggravate the concerns of MNO and 3rd parties on the data circulation. Thus, existing data sharing via network capability exposure is limited subject to the operation policy, business model and other aspects of MNO and 3rd party.
- Privacy computing can help the data flow to establish an orderly and controllable sharing mechanism, and promote the vigorous development of data elements market. Inspired by the research and application progress of privacy computing, the 3GPP exposure capability can be further enhanced by supporting the customized abstracted data sharing based on the negotiated policy between MNO and 3rd party.




- With such exposure enhancement, the various data sharing requirements from 3rd parities can be fulfilled subject to MNO policy. Therefore, 3rd party and operator could achieve a win-win situation:
  - 3rd party could deliver high-end, smarter and more convenient services to ends users with low cost;
  - MNO could deliver more added-value services to 3rd parties;
  - MNO can operate networks more efficiently and deliver better communication service to end users

# Use case 1 for Tele-operated Autonomous Driving(1)

vivo

- Regarding Tele-operated Autonomous Driving, in order to take suitable action(s) in time e.g. adjust auto-drive level to improve automatic driving safety, automaker AF need input data(X1, X2) to make a joint prediction $f_2=(f_1(X1), X2)$ about network QoS quality change and car environment change
  - Input data $X_1$ (list but not exhaustive) from operator in Table 1 as defined in 6.9, TS 23.288 and 6.20 in TR 23700-81
  - Input data $X_2$ (list but not exhaustive) from automaker AF and vehicle car in Table 2
- On demand data exposure (in the form of $f_1(X1)$) is a unique need from automaker AF as each automaker AF has its own algorithm/Model, which requires specific data exposure , hence pre-defined data exposure can not meet the requirement
- At the same time, on demand data exposure also meet the operator data sharing policy subject to data privacy

Table 1: input data $X_1$ from operator

| Information | Source | Description |
|---|---|---|
| RAN UE Throughput | OAM TS 28.554 | Average UE bitrate in the cell per timeslot, per cell, per 5QI. |
| QoS flow Retainability | OAM TS 28.554 | Number of abnormally released QoS flows during the time the QoS Flows were used per timeslot, per cell, per 5QI and per S-NSSAI. |
| UL/DL packet delay GTP | SMF or UPF | End-to-End measurements from UE to UPF. |
| UL/DL packet delay GTP | OAM | UL/DL packet delay measurement round trip on GTP path on N3. |
| Latency and delay of 5G networks | OAM TS 28.554 | Uplink and downlink delay of 5G network |
| UL/DL capacity GTP between UPF and NG-RAN | OAM TS 28.552 | UL/DL capacity measurement from UPF to NG-RAN based on GTP path. |
| UL/DL capacity GTP between UPF and UE | OAM TS 28.552 | UL/DL capacity measurement from UE to UPF based on GTP path. |
| UL/DL available capacity GTP between UPF and NG-RAN | OAM TS 28.552 | UL/DL available capacity measurement from UPF to NG-RAN based on GTP path. |
| UL/DL available capacity GTP between UPF and UE | OAM TS 28.552 | UL/DL available capacity measurement from UE to UPF based on GTP path. |
| xxx | xxxx | |

Table 2: input data X2 from automaker AF or vehicle

| Information | Source |
|---|---|
| Cooperative Lane Merge | Car or automaker AF |
| high density platooning | Car or automaker AF |
| Emergency Brake Warning | Car or automaker AF |
| Lane Change Warning | Car or automaker AF |
| Cross-Traffic Left-Turn Assist | Car or automaker AF |
| Weather | Car or Automaker AF or 3rd party |
| Traffic information | Car or Automaker AF |
| Driving habit of Owners | Car or Automaker AF |
| road infrastructure | Automaker AF or 3rd party |
| xxx | xxxx |

Note: (see details in LS SP-210619 from 5GAA [10])

# Use case 1 for Tele-operated Autonomous Driving(2)

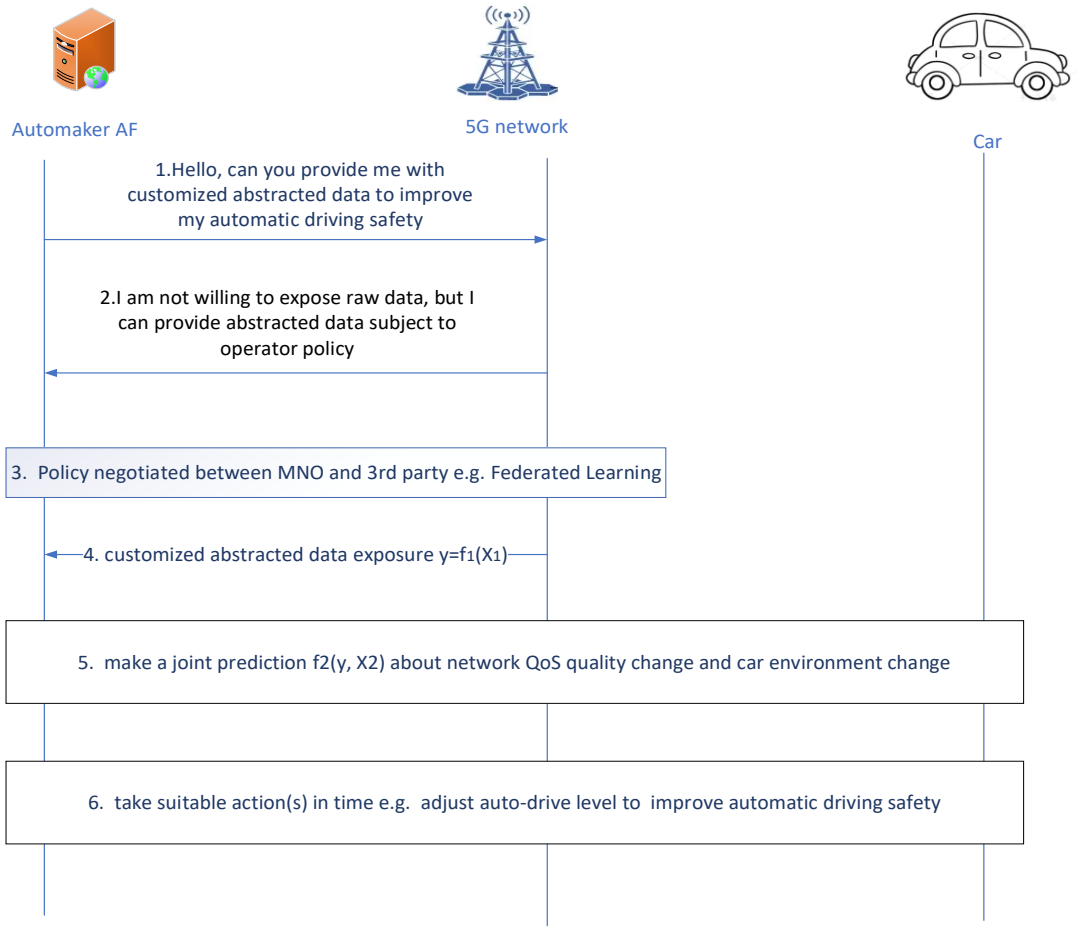
- In step 3, the policy negotiated between MNO and AF:
  - is on how to make a joint prediction:
  - contains how(i.e., y=$f_1$(x)) the MNO abstract the internal information(X1);

*Note: the policy can simultaneously meet both data sharing requirement from specific AF and MNO policy for data privacy*

- In step 4, the MNO dynamically derives the customized abstracted data y= $f_1$(X1) exposed to automaker AF

- In step 5, the automaker AF make a joint prediction $f_2$(y, X2) about network QoS quality change and car environment change.

Note: $f_2$() is AF specific algorithm, and it is out of 3GPP scope



# Use case 2 for shop location recommendation (1)

vivo

**Data owners**

**Shop owner**

Shop category, subdivided industry, time, investment, revenue status

**OTT AS**

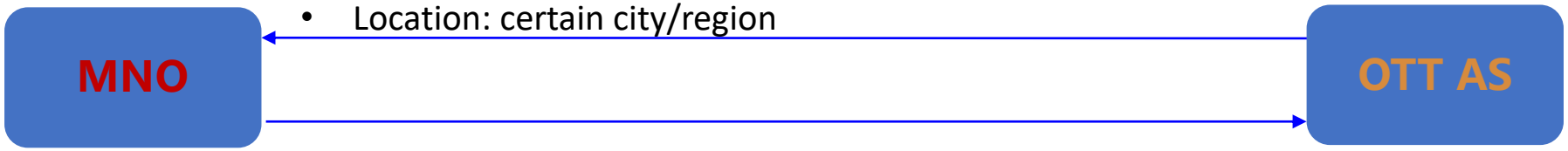
Merchant database, recommendation algorithm, takeaway revenue, user database

**MNO**

Distribution of target population, user movement track, geographical location, and moving speed

The optimization goal:

- The third party (OTT AS) determines the optimal location of the store based on the information provided by NW for the store owner's reference

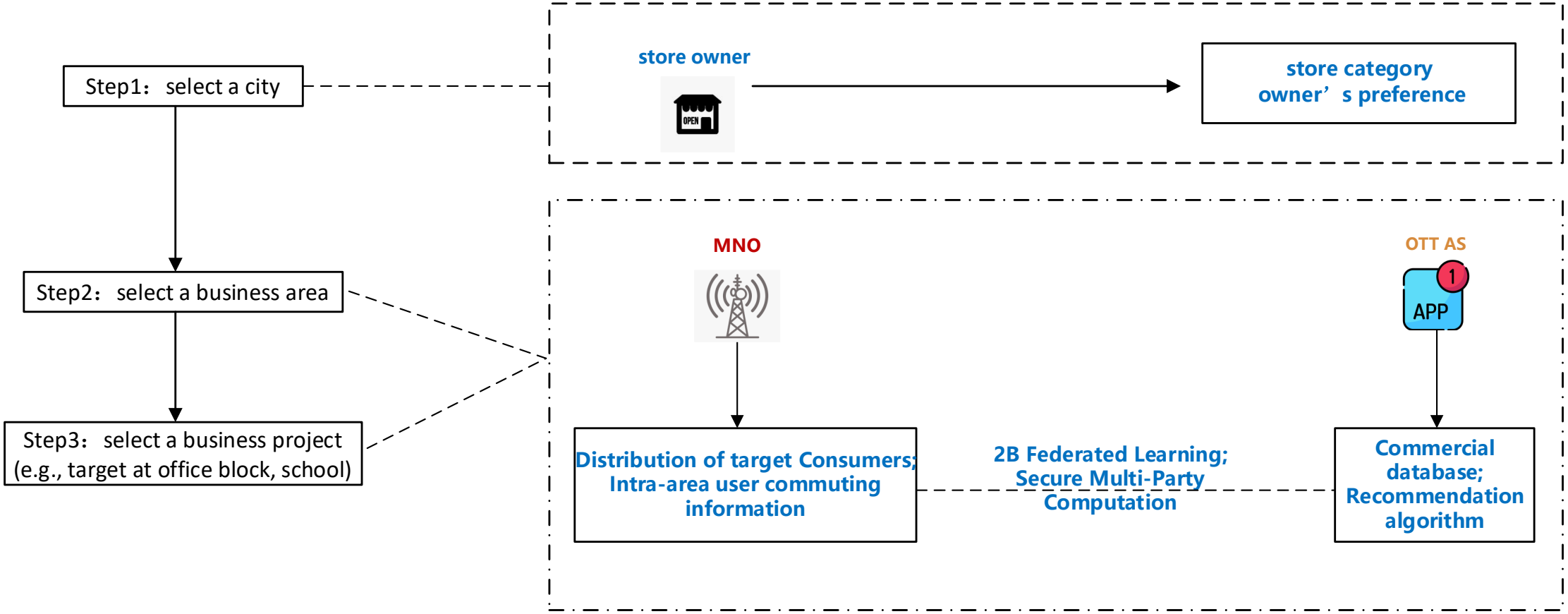



- Type for the store: a fast food/fitness/clothing store
- Type for the pricing of goods: low price/medium price/luxury price
- Location: certain city/region

- Passenger flow statistics (time period, number of people, direction, rate, etc.);
- Statistics of users' packages (proportion and number of people over 100 yuan or 200 yuan)

Note: the information from MNO can be abstracted in different granularities

# Use case 2 for shop location recommendation （2）



# Use case 3 for Joint optimization by 5GS and 3rd party AS

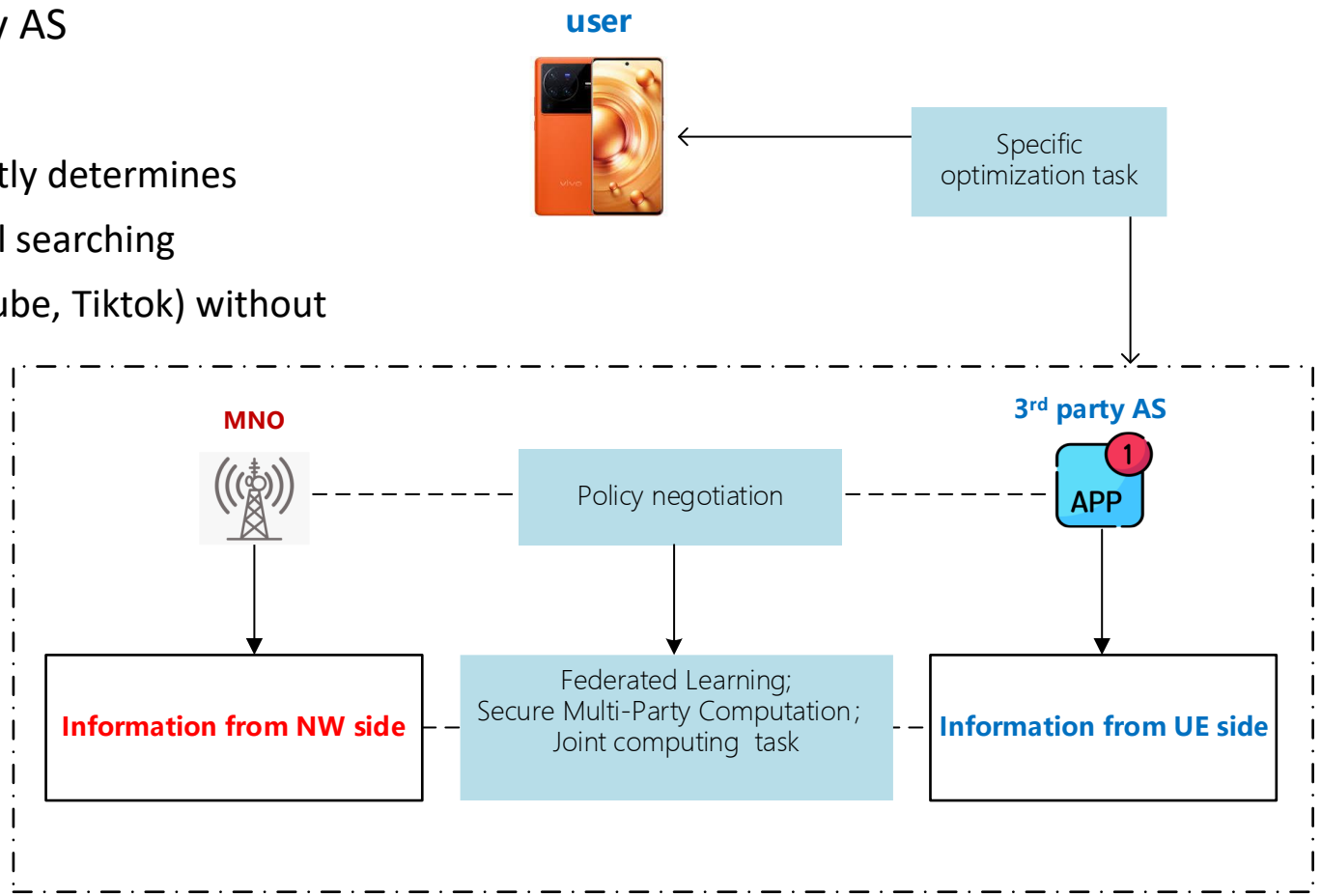
## The optimization goal:

a future value that can be used to improve user communication service experience is derived:

- by jointly computation task; and
- based on data sharing between 5GS and 3rd party AS

## Example for joint optimization :

- For areas with limited 5G coverage, the two parties jointly determines
  - strategy for inter-RAT, inter-frequency mobility cell searching
  - strategy for video streams buffering (Netflix, YouTube, Tiktok) without interruption
- Info from 3rd party side(that collected data from UE):
  - RSRP measurement results
  - Frequency/cell ID(s) of the measured cell
- Info from network side:
  - Deployment/coverage data from the network side



# Proposal

With proper abstraction of critical information exposed, the third party and the operator would have more willingness to share data between each other and provide better user service experience.

It is proposed to:

- approve the mini WID and update SA1 specification to support network exposure capability enhancement：
  - Based on operator policy, the 5G system shall provide means to negotiate with a trusted third-party the policy for customized abstraction data exposure.
  - Based on operator policy, the 5G system shall enhance data exposure (framework)capability to expose customized abstracted data to 3rd party without data privacy exposure.
  - Based on operator policy, the 5G system shall be able to provide suitable and secure means to enable an authorized third-party to provide the 3GPP network with the data analytics expected from the 3GPP network.
  - Based on operator policy, the 5G system shall be able to provide secure means for providing data analytics to authorized third-party.

  *Note: the data analytics exposure is supported in SA2 since R16 however the requirement is missing from SA1(highlighted in yellow) and it is open to whether capture it in SA1 in R19.*

# Reference


[1] Goldberg I, Wagner D, Brewer E. Privacy-enhancing technologies for the internet[C]//Proceedings IEEE COMPCON 97. Digest of Papers. IEEE, 1997: 103-109.
Privacy-enhancing technologies for the Internet.pdf

[2] https://security.googleblog.com/2019/06/helping-organizations-do-more-without-collecting-more-data.html

[3] https://ai.facebook.com/blog/crypten-a-new-research-tool-for-secure-machine-learning-with-pytorch/

[4] https://www.arm.com/en/technologies/trustzone-for-cortex-m

[5] https://github.com/secretflow/secretflow

[6] https://www.intel.com/content/www/us/en/architecture-and-technology/software-guard-extensions.html

[7] Artail, H., & Farhat, R. (2014). “A privacy-preserving framework for managing mobile ad requests and billing information.” IEEE Transactions on Mobile Computing, 14(8), 1560-1572.

[8] Daza, Vanesa, et al. "Trustworthy privacy-preserving car-generated announcements in vehicular ad hoc networks." IEEE Transactions on Vehicular Technology 58.4 (2008): 1876-1886.

[9] Roland Rieke, Maria Zhdanova, Jürgen Repp, Romain Giot and Chrystel Gaber, " Fraud Detection in Mobile Payments Utilizing Process Behavior Analysis “, 2013 International Conference on Availability, Reliability and Security

[10] LS SP-210619 from 5GAA, https://www.3gpp.org/ftp/tsg_sa/TSG_SA/Workshops/2021-09-09_Rel-18_Workshop/Docs/SP-210619.zip