



ATIS-I-0000043

ATIS Big Data Analytics Focus Group: BDA Data Value Chain Reference Model & Use Cases

October 2013



As a leading technology and solutions development organization, ATIS brings together the top global ICT companies to advance the industry's most-pressing business priorities. Through ATIS committees and forums, nearly 200 companies address cloud services, device solutions, emergency services, M2M communications, cyber security, ehealth, network evolution, quality of service, billing support, operations, and more. These priorities follow a fast-track development lifecycle — from design and innovation through solutions that include standards, specifications, requirements, business use cases, software toolkits, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). ATIS is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of oneM2M, a member and major U.S. contributor to the International Telecommunication Union (ITU) Radio and Telecommunications sectors, and a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit < www.atis.org >.

Notice of Disclaimer & Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

NOTE - The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. By publication of this standard, no position is taken with respect to whether use of an invention covered by patent rights will be required, and if any such use is required no position is taken regarding the validity of this claim or any patent rights in connection therewith. Please refer to [http://www.atis.org/legal/patentinfo.asp] to determine if any statement has been filed by a patent holder indicating a willingness to grant a license either without compensation or on reasonable and non-discriminatory terms and conditions to applicants desiring to obtain a license.

The *ATIS Big Data Analytics Focus Group: BDS Data Value Chain Reference Model & Use Cases* was developed for the **Technical and Operations (TOPS) Council**.

Published by
Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

Copyright ©2013 by Alliance for Telecommunications Industry Solutions
All rights reserved.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher. For information contact ATIS at 202.628.6380. ATIS is online at < <http://www.atis.org> >.

Printed in the United States of America.

Table of Contents

1	MOTIVATION	1
1.1	BIG DATA ANALYTICS IS A MARKET REALITY	1
1.2	REVENUE IS BEING LOST	1
1.3	CHALLENGES AHEAD	1
1.4	WHY ATIS?	2
1.5	THE WILD WEST.....	2
1.6	THE BUSINESS ECOSYSTEM.....	2
1.7	KEY GOALS OF THE BDA INITIATIVE	2
1.8	TIME IS RUNNING OUT	3
2	FINDINGS & RECOMMENDATIONS	3
2.1	OBSERVATIONS OF THE BIG DATA ANALYTICS LANDSCAPE	3
2.2	METHODOLOGY OF THE BDA FG	4
2.2.1	<i>MetaData Framework Elements</i>	<i>4</i>
2.2.2	<i>Use Cases</i>	<i>4</i>
2.2.3	<i>Privacy & Security.....</i>	<i>4</i>
2.3	ACCELERATING BDA ADOPTION.....	5
2.4	FUTURE OF BDA STANDARDS	5
2.5	AREAS OF FUTURE STUDY	5
2.5.1	<i>Provenance.....</i>	<i>5</i>
2.5.2	<i>Privacy</i>	<i>5</i>
2.5.3	<i>Cross-Industry Collaboration</i>	<i>6</i>
3	BACKGROUND	6
4	TERMINOLOGY.....	7
4.1	GLOSSARY	7
4.2	ACRONYMS	7
5	DATA SHARING VALUE CHAIN	7
6	HIGH-LEVEL USE CASES.....	8
6.1	NO SHARING USE CASES.....	8
6.1.1	<i>No Sharing: Network Operator Targeted Advertising High-Level Use Case.....</i>	<i>8</i>
6.2	LIMITED SHARING USE CASES: SHARING OF ANONYMIZED/AGGREGATED DATA.....	9
6.2.1	<i>Limited Sharing: Market Research Data Value Chain</i>	<i>9</i>
6.2.2	<i>Limited Sharing: Improving Relevance of Real-Time Ads.....</i>	<i>9</i>
6.3	FULL PII SHARING: SHARING OF PERSONAL IDENTIFIABLE INFORMATION (PII)	10
6.3.1	<i>Full PII Sharing: One-to-One Targeted Advertising via SMS Messages.....</i>	<i>10</i>
7	DATA VALUE CHAIN REFERENCE MODEL	10
7.1	RETAINER REQUESTOR REFERENCE MODEL.....	10
7.2	BDA METADATA MODEL	12
7.2.1	<i>Acceptable Use & Privacy Policy Concepts.....</i>	<i>13</i>
7.2.2	<i>Retainer Requestor Concepts</i>	<i>16</i>
	<i>Name.....</i>	<i>18</i>
	<i>Description.....</i>	<i>18</i>
	<i>Enumeration Literals</i>	<i>18</i>
7.2.3	<i>Context (Jurisdiction, Locations, Date/Time).....</i>	<i>20</i>
7.3	PARTICIPANTS (ACTORS/ROLES/ORGANIZATION)	22

7.4	PARTICIPANT DATA MODELS	25
7.4.1	<i>Network Operator Data Model</i>	25
7.4.2	<i>Mobile Gaming App Company Data Model</i>	27
7.4.3	<i>Advertiser Data Model</i>	28
8	EXAMPLE USE CASES	31
8.1	FULL PII SHARING: MOBILE GAMING USE CASE	31
8.1.1	<i>Mobile Gaming Use Case: Sharing Request</i>	31
8.1.2	<i>Mobile Gaming Use Case: Data Sharing Request Detail</i>	31
8.1.3	<i>Mobile Gaming Use Case: Data Processing Detail</i>	32
8.1.4	<i>Mobile Gaming Use Case: Data Sharing Response Detail</i>	33
8.1.5	<i>Mobile Gaming Use Case: SMS Advertisements</i>	33
8.1.6	<i>Mobile Gaming Use Case: Retainer Metadata Population</i>	35
8.2	LIMITED SHARING: IMPROVING RELEVANCE OF REAL-TIME ADS USE CASE	41
9	COLLABORATIONS	42
9.1	COLLABORATION PARTICIPANT CONVERSATIONS	42
9.1.1	<i>Participant Conversations</i>	42
9.2	COLLABORATION SUBSCRIBER NETOP COLLABORATION	42
9.2.1	<i>Subscriber NetOp Collaboration</i>	43
9.3	COLLABORATION DATA PARTNER COLLABORATION	43
9.3.1	<i>Data Partner Collaboration</i>	43
9.4	COLLABORATION PER SUBSCRIBER ACTION REQUEST COLLABORATION	44
9.4.1	<i>Per Subscriber Action Request Collaboration</i>	44
10	PROCESSES	44
10.1	PROCESS POPULATE META-MODEL	45
10.1.1	<i>Process Elements</i>	47
10.2	PROCESS P37 POPULATE META-MODEL	50
10.2.1	<i>Process Activities:</i>	51
10.3	SERVICE SUBSCRIPTION & USAGE PROCESS DEFINITION	53
10.3.1	<i>Process Wireless Service Subscription</i>	53
10.3.2	<i>Process Collect Subscriber Data</i>	54
10.3.3	<i>Process Voice Usage</i>	56
10.3.4	<i>Process Mobile Data Usage</i>	58
10.3.5	<i>Process Mobile App Usage</i>	59
10.4	PROCESS DATA	61
10.5	PROCESS SHARED DATA REQUESTS	61
10.6	PROCESS ACQUIRE RELATED PARTNER SHARED DATA	61
10.7	PROCESS SEND SMS	61
10.8	PROCESS ASSUME THE RETAINER ROLE FOR SHARED DATA	62
10.9	PROCESS STORE OUTPUT RECORDS	62
10.10	PROCESS SERVE SHARED DATA REQUESTS	62
10.11	PROCESS SERVE ACTION REQUESTS	63
10.11.1	<i>Elements descriptions:</i>	63
11	ACKNOWLEDGEMENTS	64
12	SOURCES	64

Table of Figures

FIGURE 1: DATA SHARING VALUE CHAIN	8
FIGURE 2: RETAINER-REQUESTOR REFERENCE MODEL	11
FIGURE 3: META-MODEL DATA DIAGRAM	13
FIGURE 4: BDA RETAINER-REQUESTOR MODEL	16
FIGURE 5: RETAINER-REQUESTOR SHAREABLE DATA RECORD LIST MESSAGES	19
FIGURE 6: CONTEXT DEFINITION CONCEPTS	20
FIGURE 7: TIME CONTEXT DATE OF THE WEEK	22
FIGURE 8: TYPICAL PARTICIPANT ORGANIZATIONAL ROLES	23
FIGURE 9: TYPICAL NETWORK OPERATOR DATA MODEL	25
FIGURE 10: TYPICAL MOBILE GAMING COMPANY DATA MODEL	27
FIGURE 11: TYPICAL ADVERTISER DATA MODEL	28
FIGURE 12: AD CAMPAIGN REQUEST	30
FIGURE 13: MOBILE GAMING USE CASE - SHARING REQUEST	31
FIGURE 14: MOBILE GAMING USE CASE - DATA SHARING REQUEST DETAIL	32
FIGURE 15: MOBILE GAMING USE CASE - DATA PROCESSING DETAIL	32
FIGURE 16: MOBILE GAMING USE CASE - DATA SHARING RESPONSE	33
FIGURE 17: MOBILE GAMING USE CASE - ADVERTISING TO TOP MOBILE GAMERS (RETAIN INPUT RECORDS)	34
FIGURE 18: MOBILE GAMING USE CASE - REQUESTOR VERIFIES SHARING POLICIES	34
FIGURE 19: MOBILE GAMING USE CASE - SMS ADVERTISEMENTS ACTION REQUESTS/TEXT MESSAGE ADS	35
FIGURE 20: EXAMPLE METADATA MODEL POPULATION FOR JURISDICTIONAL CONTEXT	36
FIGURE 21: EXAMPLE METADATA MODEL POPULATION FOR CONTEXT & ACCEPTABLE USE POLICY	37
FIGURE 22: EXAMPLE METADATA MODEL POPULATION OF SHARED DATA RECORDS AND ATTRIBUTES	38
FIGURE 23: COMPLETE POPULATION OF METADATA	39
FIGURE 24: MOBILE GAME ADVERTISEMENT	40
FIGURE 25: RELEVANCE OF REAL TIME ADS EXAMPLE	41
FIGURE 26: DATA PARTNER COLLABORATION	42
FIGURE 27: DIAGRAM SUBSCRIBER NETOP COLLABORATION	42
FIGURE 28: DATA PARTNER COLLABORATION	43
FIGURE 29: PER SUBSCRIBER ACTION REQUEST COLLABORATION	44
FIGURE 30: RETAINER-REQUESTOR PROCESS DEPENDENCIES	45
FIGURE 31: POPULATE META-MODEL ACTIVITY DIAGRAM	46
FIGURE 32: PROCESS TO POPULATE META-MODEL	51
FIGURE 33: WIRELESS SERVICE SUBSCRIPTION	53
FIGURE 34: COLLECT SUBSCRIBER DATA ACTIVITIES	54
FIGURE 35: VOICE USAGE	57
FIGURE 36: MOBILE DATA USAGE	58
FIGURE 37: MOBILE APP USAGE	60
FIGURE 38: SERVE ACTION REQUIREMENTS	63

Table of Tables

TABLE 1: META-MODEL CONCEPTS TERMINOLOGY	14
TABLE 2: META-MODEL CONCEPT ENUMERATIONS	15
TABLE 3: BDA RETAINER-REQUESTOR TERMINOLOGY	16
TABLE 4: BDA RETAINER-REQUESTOR CONCEPT ENUMERATIONS	18
TABLE 5: CONTEXT AWARE TERMINOLOGY	20
TABLE 6: CONTEXT ENUMERATIONS	21
TABLE 7: DATA PARTNER ORGANIZATIONS	22
TABLE 8: TYPICAL PARTICIPANT ORGANIZATIONAL ROLE DESCRIPTIONS	24
TABLE 9: NETWORK OPERATOR DATA MODEL TERMINOLOGY	26
TABLE 10: AD CAMPAIGN REQUEST MESSAGE DESCRIPTION	30

ATIS Big Data Analytics Focus Group: BDA Data Value Chain Reference Model & Use Cases

1 Motivation

1.1 Big Data Analytics is a Market Reality

The buzz around Big Data Analytics has raged for the past few years. Articles on the subject have permeated mainstream media, heralding an edge to vault past competitors by applying sophisticated data mining techniques on the exploding volume of digital data generated by countless devices and sensors. The promise of course is that this will create insight – previously unknown information – to help business make data-driven decisions.

Three factors have combined to make Big Data Analytics a reality. The price of storage has fallen precipitously, processing power has increased enormously and the amount of data being created by networks, applications, and devices has grown to an exabyte every day. Capturing and analyzing this data has become a very robust business in a very short time: \$12 billion this year alone.

Communications service providers (CSPs) who are able to collect and analyze the wealth of network, customer and location data can use this information in many ways, including differentiating their services, offering location-based services, creating targeted marketing campaigns, improving network performance, detecting fraud, and reducing costs.

1.2 Revenue is Being Lost

Today, however, CSPs are not able to fully make use of the data generated by their subscribers. Instead, it is the over-the-top players who have been able to capitalize on Big Data Analytics and who are taking the lion's share of the revenue opportunities this activity creates. For example, 90 percent of mobile advertising revenue is going to OTT players – 70 percent to Google and Facebook alone – and the percentage available to CSPs is shrinking, not growing.

CSPs looking to leverage this data face several obstacles. First of all, accessing and processing the wide variety of information generated is difficult because it is often captured and maintained in different organizational silos within a service provider, often in different physical locations. Making the task more difficult is the fact that most CSPs are creating proprietary, home-brew Big Data Analytics solutions. There are, however, some indications that cooperation and collaboration is beginning, as the examples of WEVE in UK, Sprint, and Telefonica illustrate.

Mobile advertising appears to be a leading means to monetize this analytic insight, but there are many other interesting use cases. For example, Verizon Wireless works with athletic teams and sports venues to map where attendees live in order to increase awareness in underrepresented neighborhoods. Telefonica works with local communities to understand traffic impacts of local events and late night shopping for improved planning.

1.3 Challenges Ahead

If the telecommunications industry as a whole wants to benefit from the power of Big Data Analytics, then the following major challenges must be overcome. First, there is no coordinated effort or industry standard. This makes progress very slow, as everyone starts working from scratch, information is kept very close to the vest and no best practices can emerge for others to learn from. Secondly, the individual, siloed approach described above prevents the creation of a comprehensive, industry-wide view. Third, external entities who value this data for their own purposes don't want to be restricted to one CSP's information, and they also don't want to have to deal with multiple incompatible datasets. We envision the rise of analytics aggregators – similar to what we see in the financial services – that can combine information across multiple CSPs, and possibly contribute a value-added service powered by their analytics.

Finally, and perhaps most importantly, the general public harbors significant concern about privacy and data security, which have only been exacerbated by recent revelations about the extent of data being collected by both

government and commercial entities. CSPs who seek to leverage subscriber data must be mindful of both customer backlash and government legislation (witness any time Facebook changes its terms of service).

1.4 Why ATIS?

ATIS is a representative and advocate for communication service providers. It is an independent body that helps establish best practices, guidelines and standards in an industry that is growing rapidly and facing constant change. The explosion of data services is an example of this change, but understanding how to manage this data is still a work in progress for many CSPs. By bringing people together from various organizations across the industry, ATIS is able to provide a collaborative setting for putting standards in place that helps the industry as a whole respond to this change more effectively.

1.5 The Wild West

In the financial world, there are companies in place that gather data on payment histories of both individuals and enterprises. Companies like Experian, TransUnion, and TRW gather information from a national network of retailers, banks, utilities and others to create individual credit scores which are used to help businesses and banks make better business decisions. These are trusted organizations that adhere to strict standards and security protocols. A person or a business with a good credit score benefits by paying lower interest rates and the banks benefit by lowering their risk of bad debt. In other words, both parties usually benefit in some way by sharing this information.

In the communications world, service providers are finding themselves with a wealth of data that they have never had before, but without a guidebook in place for how to manage it. We are in the 'Wild West' of Big Data – where business rules and regulations haven't kept pace with technology. This is where ATIS can help. We believe that establishing a set of industry guidelines and standards will help to mitigate future problems related to issues such as privacy and transparency, and create a more trusting relationship between CSPs and their subscribers.

1.6 The Business Ecosystem

Business ecosystems are quickly forming to take advantage of valuable subscriber data. Communication Service Providers, Data Aggregators, Advertisers, Businesses, Brands, and even the Federal Government, are all in the Big Data Gold Rush of today. But without standards in place, each organization is working in a silo -- without a roadmap or rulebook for how to navigate in this new world. Mistakes are being made, and people's perceptions about data, privacy, and fairness are being defined in a negative manner. We believe that now is the time to address these issues head on.

Standards will facilitate broader insight useful for many entities. For CSPs, the richness of data at their fingertips represents a sizeable new revenue stream. But beyond the operators, analytics generated from the communication networks potentially creates new business models to enable a broader ecosystem. Mobility, customer behavior, subscriber location, social networks and other insights become even more valuable when combined with data from other industries for advertisers, retailers, aggregators, hospitality, security players, and others. Such an ecosystem is likely to usher in new entrants driven by an information economy.

1.7 Key Goals of the BDA Initiative

ATIS can help the communications industry reach a consensus on three key data-related issues that need to be addressed and defined:

- What is the information we are gathering?
- Where is it coming from?
- How are we allowed to use it?

'What' works to describe the data being exchanged? Are there any parameters or guidelines that need to be put into place? Does this information represent an individual, family, account, or enterprise? Are the metrics within the data native information, aggregated, or derived? What is the level of confidence in the data set?

'Where' defines the provenance of the data. What is the source of the data? What was the history of ownership? How was the data processed, refined, or enriched over its ownership history? Which service providers will participate, and which third parties will contribute?

And lastly, 'How' describes what rules need to be defined around use of this data. Are there uses and applications that will not be allowed? How will Opt-in requests be managed? Should the data be aggregated and 'anonymized'? How can the process be made transparent to subscribers? How will the CSPs derive value from this ecosystem, and pass on that value to opted-in subscribers? What are the 'right to use' and acceptable use' policies? What data can be shared, and what data can't be shared – and how will this be communicated and enforced?

The Importance of Trust

Due to the recent news about data collection and the National Security Agency, it is worth noting that one of the biggest pain points from an outside perspective was the lack of transparency. Without transparency, without communication, people assume the worst.

We all want to be able to control our own destiny, including our digital destiny. By putting the rules, regulations, and parameters in place at an industry level to address these issues head on, the communications industry will be able to build healthier relationships with its subscribers and create a path for a big data ecosystem that will benefit all the players involved.

1.8 Time is Running Out

These questions and more will need to be addressed quickly. Technology isn't slowing down, and the issues of data use, privacy, ownership, and transparency will not go away. This is why the ATIS BDA project is so important.

The ability to create an audit trail of data and build a community of trust will be critical for our industry, our business, and our subscribers. It is up to our industry to help protect consumers from illegal or intrusive use of their personal data, while at the same time protecting the ecosystem players that want to use the data in a lawful and transparent manner.

2 Findings & Recommendations

2.1 Observations of the Big Data Analytics Landscape

As the Big Data Analytics Focus Group wraps up its study, an overarching reality check is that while BDA has become a mainstream goal in the communications industry, the sharing of analytics insight with multiple parties is in its nascent stages. CSPs are at different maturity levels of applying BDA to monetize their information assets, although several are working at advanced levels.

However, it is apparent that even those operators pursuing advanced applications are doing so in a proprietary manner. In many ways, this reflects the early stages of applying analytics to monetize data assets. Secondly, analytics and the underlying data, algorithms, and models are likely viewed as competitive differentiators; CSPs in the early stages may not be in a position, or willing, to generalize or share their approach lest they lose their competitive edge. Yet such an approach is only possible for the largest operators with the scale, budget, and clout to shape their ecosystem.

This "big stick" approach brings to mind Wal-Mart's 2002 mandates to its suppliers in the early days of internet commerce. By mandating electronic data standards, Wal-Mart pioneered secure internet-based supply chain automation. Few suppliers could afford not to do business the "Wal-Mart Way" if they wanted to work with the world's largest retailer. For Wal-Mart, this heralded further efficiencies in its already impressive processes. But for suppliers, it meant additional significant IT costs to work with Wal-Mart, using a process which was unlikely to

work with other retailers. Yet, one of the results of such initiatives was to change the competitive landscape, forcing other retailers to create processing frameworks to improve their own supply chains. The existence of multiple frameworks accelerated the adoption of data exchange standards.

In much the same way, proprietary BDA approaches by larger operators have the potential to create mutually beneficial ecosystems that leverage insight generated by Big Data Analytics – mobility, customer behavior, subscriber location, social media activity, and other insights – to create new revenues. However, it also creates IT burdens for ecosystem players and islands of incompatible ecosystems.

2.2 Methodology of the BDA FG

The nascent nature of BDA makes the definition of a standard premature. The BDA Focus Group understands that development of standards take time. However, a side effect of our work is the identification of common terminology, typical use cases, best practices, most appropriate technologies, and emerging developments. We believe interim results and guidelines help reduce the fragmented approaches currently seen within the frenzied and rapidly evolving analytics market.

By studying how analytics are applied in the industry, the team found common themes. Understanding that a standard was unlikely in the short term, we nonetheless created a framework with elements and concepts that we believe are necessary for any future standard.

2.2.1 MetaData Framework Elements

- *Metadata Model* – 7.2 describes a data partner's typical data model and context-aware acceptable use policy. A metadata model that records everything about a describing a data partner's data records, attributes, acceptable use policies, opt-in preferences, etc.
- *Retainer Requestor Model* – 7.1 and 7.2.2 provide alternative views of the metadata model which describe the origin and collective processing applied to arrive at the insight.
- *Participants* – 7.3 shows the typical stakeholders and internal organizational roles.
- *Common Data Models* – 7.4 presents the typical data models for the relevant data partners.
- *Collaborations* – 9 includes interactions among the data partners in BPMN2 collaboration diagrams.
- *Processes* – 10 describes the processes models as BPMN2 processes.

2.2.2 Use Cases

The team defined three high-level use cases, enumerated below, and discussed further in Section 6. These use cases exhibit varying degrees of privacy concerns, and the number of relevant actors. The use cases are:

- Operator targeted advertising (no sharing);
- Sharing of anonymized, aggregated data (limited sharing); and
- Sharing of personal identifiable information (PII) (full sharing).

We then applied the framework to these use cases as a concrete example of how to model, esnruign the framework was robust enough, for the typical application areas.

2.2.3 Privacy & Security

A significant area of investigation focused on privacy and security issues. As a result, the metadata to describe the privacy and security policy of how the data may (and/or may not) be used was incorporated into the following concepts in the reference model:

- Acceptable Use and Privacy Policy Concepts (7.2.1).
- Opt-In/Opt-Out Preferences (7.2).
- Context (Jurisdiction, Locations, Date/Time) (7.2.3).

2.3 Accelerating BDA Adoption

To advance the maturity of “Data Value Chain” BDA, the FG recommends the following:

- Complete modeling of more complex use cases to exercise the framework;
- Define and develop a communications-specific analytics sandbox. This environment would contain anonymized customer and/or network data for the purpose of prototyping analytics algorithms and metadata; and
- Implement non-shared BDA applications (such as network analytics for operational efficiency) to exercise the framework.

2.4 Future of BDA Standards

It is clear that the use of BDA will continue to evolve; part of the maturation process will be the widening of the Data Value Chain. While the focus of this group has been around the CSPs as the owners of the data, the broader Data Value Chain will include many other players that take data from the operators, add value to the data by processing, enriching, or further transforming it. Conversely, data from these other players may flow back to operators, effectively making CSPs both owners and requestors.

Ultimately, BDA is destined to become Data as a Service. There are already well known examples – typically internet players – with Data-as-a-Service business models that monetize analytic insight. Such examples include:

- Facebook – social interaction;
- Google Maps, Waze – navigation and traffic patterns;
- Amazon – purchase behavior; and
- Netflix – movie viewing behavior and preferences.

2.5 Areas of Future Study

The BDA Focus Group considered two notable topics, data provenance and privacy, for inclusion in the BDA Data Value Chain reference model.

2.5.1 Provenance

Provenance is “the origin or source of something¹”. The origin of the data is important in the areas of data ownership, monetization, and protecting a subscriber’s privacy. While this document current takes into account these requirements, it is possible that the W3C’s PROV-DM could serve as a foundation for the owner-requestor model view. In the future, if the PROV-DM model is widely adopted in Data Value Chains, it would be advantageous to serialize the owner-requestor model in a PROV-DM view for the purposes of exchanging data provenance.

2.5.2 Privacy

Historically anonymization, and pseudonymization techniques have been used to mask PII data by redacting values or mapping those values to a different set of values prior to data release. More recent techniques, such as Differential Privacy seek to maximize the utility of an aggregate data set while reducing the risk of re-identification.² However, aggregation of multiple data sets and correlation techniques may still allow re-identification. In particular, higher resolution CSP location information combined with publicly available address information can provide a significant set of data points that increase the risk of re-identification.

¹ Merriam-Webster Learner's Dictionary

² (Dwork, 2008)

Re-identification science exposes the underlying promise made by [anonymization] laws—that anonymization protects privacy—as an empty one, as broken as the technologists’ promises.³ - Paul Ohm, Broken Promises Of Privacy

Privacy law and regulation is in a state of disruption due to privacy research focused on preventing re-identification techniques while maximizing utility data release. Privacy preserving algorithms are expected to change at a rapid rate as privacy law and re-identification research mature. As such, data processing is represented in the Owner-Request Model with an option for privacy-related transformations of the data to extend and specialization of a general metadata model.

In a *UCLA Law Review* article, Paul Ohm argues that anonymization is nothing more than a “release-and-forget” model, not to mention, ubiquitous and flawed.⁴

The relative maturity of standards to enable a user (original source of data) to maintain control of data collected by Service Providers can vary depending on the Use Case and industry segments (verticals) involved. In the case of eHealth and electronic health records, significant work has already been done on modeling and metadata definitions in eHealth SDOs such as HL7, driven by patient privacy laws and regulations. However, it is not clear whether a common privacy framework across multiple industry segments is achievable, or optimal. Such a multi-segment BDA Privacy Framework gap analysis was not possible in the BDA FG timeframe.

2.5.3 Cross-Industry Collaboration

There are important cross-industry considerations as next steps are evaluated. The telecom-specific modeling provides a depth that may be useful to other industry groups. As other industries move to data exchange and mobile delivery channels, the BDA Metadata Model may lend a technical communications perspective to other domains.

3 Background

Network operators possess a rich set of detailed information about their customers enabling a host of analytics capabilities such as behavioral, location-based, and customer experience analytics. However, over-the-top (OTT) providers are monetizing customer data at the app level through advertising and mobile app sales at the expense of the network operator. Simultaneously, mobile customers are seeking to reduce their monthly spending and are usually willing to share personally identifiable information (PII) in return for reduced fees or increased usage levels.

Privacy and security of customer data in the U.S. are of utmost concern to the general public. According to a recent WSJ article⁵, several wireless carriers around the globe have begun “to sell the vast troves of data they gather about their subscribers’ locations, travels and Web-browsing habits.” While, many U.S. citizens are opposed to the National Security Agency’s phone records collection program, House lawmakers voted down a bill that would have significantly reduced the NSA program⁶. At present, U.S. network operators are sharing data as they please while adhering to privacy policies agreed upon by their subscribers. Network operators have an interest in lobbying our lawmakers to ensure that privacy policy maintains a healthy balance with data utility (e.g., the monetary value or analytic usefulness of a dataset). *With the ever-changing regulatory and legal landscape for consumer privacy, network operators need a standard data sharing model that adapts to*

³ (Ohm, 2010, p. 1704)

⁴ (Ohm, 2010, pp. 1711-1712)

⁵ (Troianovski, 2013)

⁶ (Gorman, 2013)

future privacy concerns pertaining to individual subscribers and a data sharing partner's use of their data.

This document defines such a model to both enable network operators to monetize customer data through big data analytics and share data with third parties. Each data sharing partner, in the data value chain, provides additional value by combining related data from third parties and monetizing the results for consumption by other third party partners throughout the data value chain.

4 Terminology

4.1 Glossary

Glossary Term	Glossary Definition
Data Provenance	The lineage of the data throughout the Data Value Chain from its origin throughout any process that occurs along the way.
Data Value Chain	A network or ecosystem of data partners that seek to monetize data by collecting raw data and producing value-added data sets and providing services for customer engagement.
Differential Privacy	Privacy preservation techniques seek to maximize privacy of aggregate data, upon disclosure to third parties, while maintaining data utility. Privacy is preserved by minimizing the re-identification of an individual from aggregate data sets, when aggregate data about a specific individual is known (e.g., age, gender, and zip code). Differential privacy techniques originate from the statistical disclosure control theory and integrate computer science algorithms, data theory, and cryptography.
Re-identification	The identification of an individual in an aggregate data set that does not contain personally identifiable information for that individual.

4.2 Acronyms

BDA	Big Data Analytics
BPMN2	Business Process Modeling Notation 2
OTT	Over-The-Top
PII	Personally Identifiable Information
PMML	Predictive Model Markup Language
UML	Unified Modeling Language

5 Data Sharing Value Chain

An example of the data sharing value chain model is shown below depicting a typical ecosystem of data sharing partners. Data sharing partners are classified under the following roles and notated by enclosing << >>'s in the Figure below:

- Network operator;
- Related partner;
- Un-related partner; and
- Government agency.

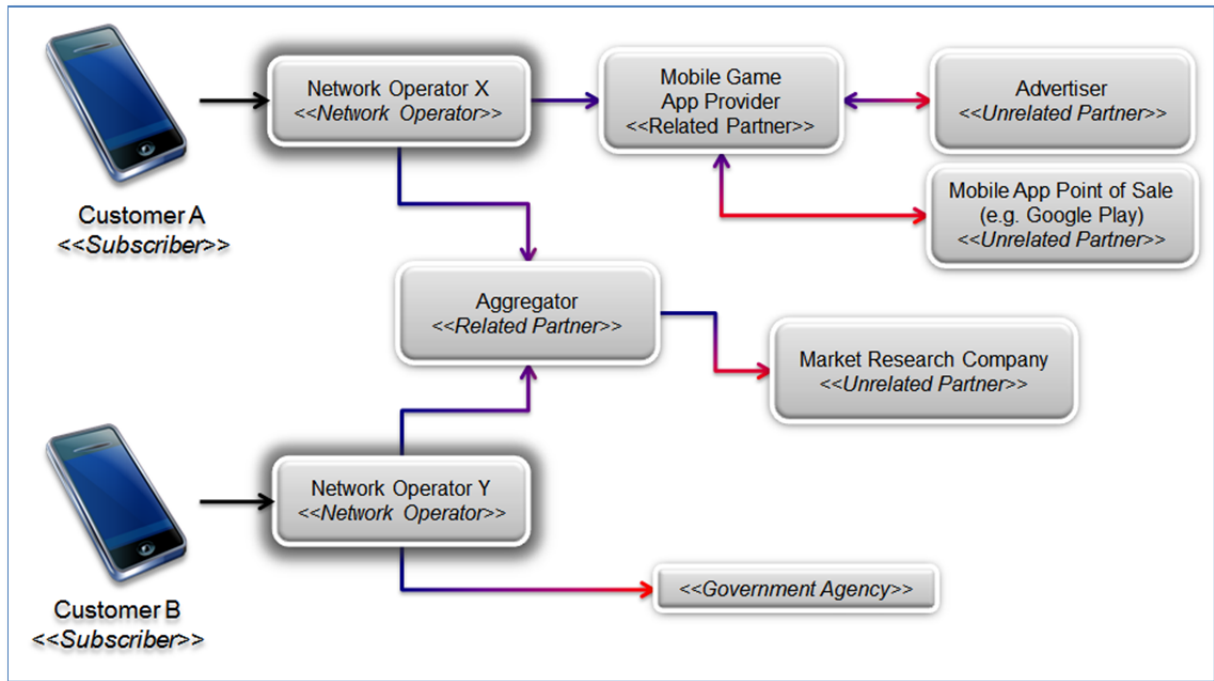


Figure 1: Data Sharing Value Chain

6 High-Level Use Cases

Three high-level use cases considered in the context of the data value chain specialized use cases are:

- Operator targeted advertising (no sharing);
- Sharing of Pseudonymized, aggregated data (limited sharing); and
- Sharing of personal identifiable information (PII) (full sharing).

6.1 No Sharing Use Cases

6.1.1 No Sharing: Network Operator Targeted Advertising High-Level Use Case

Network Operators provide targeted advertising services to a related partner without sharing any personally identifiable information (PII) with the related partner.

This use case has the following actors and roles in pertaining to the data value chain model.

Example Actor	Actor Role	Description
Network Operator X	Network Operator	Owns customer PII data and provides the ability to send target SMS or mobile notifications for advertisements on behalf of the mobile game app provider's ad campaign parameters.
Mobile Game App Provider	Related Partner	Provides the advertising message content and ad campaign parameters.
Advertiser	Un-related Partner	An advertising company with a direct relationship with the mobile game app provider who provides advertising planning services. As an un-related partner, the advertiser does not have a direct relationship with the network operator .
Mobile App Point of Sale	Un-related Partner	Shares mobile app purchasing data with the Mobile Game App Provider.

6.2 Limited Sharing Use Cases: Sharing of Anonymized/Aggregated Data

6.2.1 Limited Sharing: Market Research Data Value Chain

Actor	Role	Description
Network Operator X	Network Operator	Network Operator X provides anonymized/aggregated data to the aggregator.
Network Operator Y	Network Operator	Network Operator Y provides anonymized/aggregated data to the aggregator.
Aggregator	Related Partner	An aggregator is a related 3 rd party partner with an agreement in place with each of the network operators. Aggregators provide an anonymous and aggregated view of customers across multiple network operators. Aggregators are also in a unique position to form data sharing partners with other data partners for additional reference information that can add more value by combining other reference data sources to customer data (e.g., Census.gov/data).
Market Research Company	Unrelated Partner	A market research company is an unrelated partner with respect to the network operator. However, they may purchase aggregate/anonymous data from an aggregator and provide specific reports targeting various companies within the mobile communications industry.

6.2.2 Limited Sharing: Improving Relevance of Real-Time Ads

This use case outlines a scenario where a network operator builds a user profile based on user's browser behavior (clicks, download, upload, shopping cart) for users that opt-in. In this use case, the network operator can create an anonymized data set that is based purely on user's visit to website(s) and typical browser behavior. In this use case, the network operator shares hashed key-based user data with online marketers (offline), whereas, the website a user is visiting, the visited website can in real-time feed user browser data (with hashed keys) to send to the online marketer. This allows online marketer to match the stored hashed keys with real-time data and generate dynamic advertising.

Actor	Role	Description
Network Operator X	Network Operator	Network Operator X provides anonymized data based on user browser behavior (hashed-keys) to an online advertisement agency (DSP or DMP).
Mobile/Desktop Web User	User (Subscriber)	The web user (mobile or desktop) browser behavior is captured by Network Operator (there is no PII information provided to partners).
Online Marketer/Data Aggregator (DSP or DMP)	Related Partner	Online marketer collects anonymized user data from one or more network operator(s). The online marketer dynamically generates advertisement and serves the website by matching user hashed key stored in its DB with user hashed key provided by website.
Website	Related Partner	A user when browsing website shall be presented specific advertisement based on recent browser history and behavior.

See 8.2 for an example this use case.

6.3 Full PII Sharing: Sharing of Personal Identifiable Information (PII)

6.3.1 Full PII Sharing: One-to-One Targeted Advertising via SMS Messages

Actor	Role	Description
Mobile Device User X	User (Subscriber)	The end user of a mobile device associated with a subscriber's account opts-in to the default Acceptable Use Policy of Network Operator X and also opts-in to share PII data in return for delivery of relevant advertisements.
Network Operator X	Network Operator	Owns customer PII data and provides the ability to send targeted advertisement via SMS or mobile notifications by sharing the mobile phone number of the subscriber directly with the Mobile Game App Provider. Acquires mobile purchase history and mobile game app usage data from the Mobile Game App Provider and combines with per-subscriber data sets to deliver one-to-one advertising.
Mobile Game App Provider	Related Partner	Provides the advertising message content and ad campaign parameters. Acquires purchase history data from Mobile Game App Point of Sale. Shares purchase history and mobile app usage data with the Network Operator.
Advertiser	Un-related Partner	An advertising company with a direct relationship with the mobile game app provider who provides advertising planning services. As an un-related partner, the advertiser does not have a direct relationship with the network operator.
Mobile App Point of Sale	Un-related Partner	Shares mobile app purchasing data with the Mobile Game App Provider.

7 Data Value Chain Reference Model

7.1 Retainer Requestor Reference Model

The owner-requestor reference model presented in Figure 2 depicts a tertiary relationship among the customer, owner, and requestor.

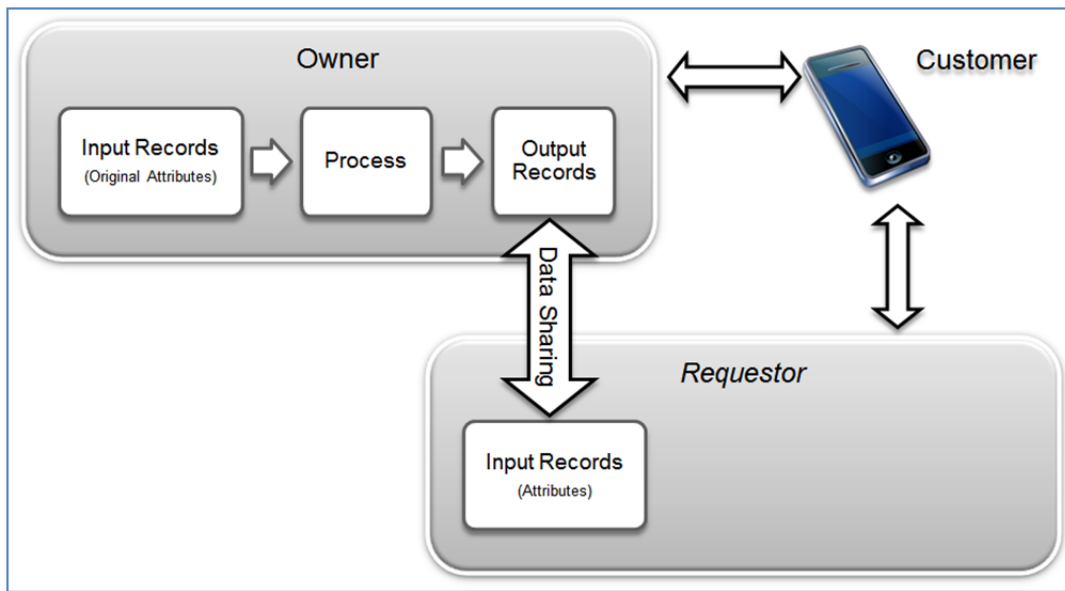


Figure 2: Retainer-Requestor Reference Model

- Customers subscribe to a network operator's service and share personally identifiable information (PII) under the agreed to privacy policies of the owner (e.g., typically the network operator). Customers may opt-in to additional services that allow for sharing of the PII data with related and/or un-related third party partners.
- Owners collect, store, process, and share customer data per the owner's privacy policy. Any data sharing partner within the data value chain may be an owner of a specific data set acquired indirectly through their partners or directly from the customer.
- Requestors acquire customer data indirectly from other data sharing partners within the data value chain. Requestors store, analyze, and produce value-added customer data typically at an anonymous/aggregate level. However, some data partners may work with per customer data for those customers who choose to opt-in to allow PII level sharing.
- Input records are specific data records and their associated attributes that are inputs to some process that generates value-added data for either internal or external use.
- Process refers to the means used to create value-added data from input records and to generate and/or store output records.
- Output records are value-added data records resulting from data processes with respect to a customer or some anonymous/aggregate of customers. An output record may be stored for future use (e.g., historical time series analysis) or it may be shared and then discarded immediately.
- Data Sharing is the process by which an owner publishes shared data metadata (e.g., metadata describing the structure of output records) and allows the actual data to be shared. The requestor then has the option to request data per their business agreement with the owner.

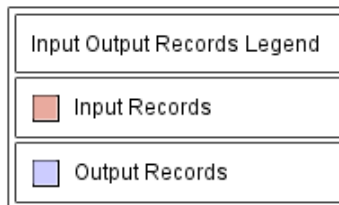
While the network operator is typically the original owner of customer specific data, any third party may become a subsequent owner by acquiring and storing the customer data.

7.2 BDA Metadata Model

The BDA metadata includes all information required about the input, processing, or output records as it applies to the data value chain including:

- Attributes of Input/Output Data Records and Attribute Groups;
- Data Processing Specifications;
- Acceptable Use and Privacy Policy Concepts;
- Context Aware Concepts; and
- Retainer / Requestor Model Concepts.

Note: The Input Output Records Legend is used throughout this document to show which records are associated with Input Records or Output Records.



7.2.1 Acceptable Use & Privacy Policy Concepts

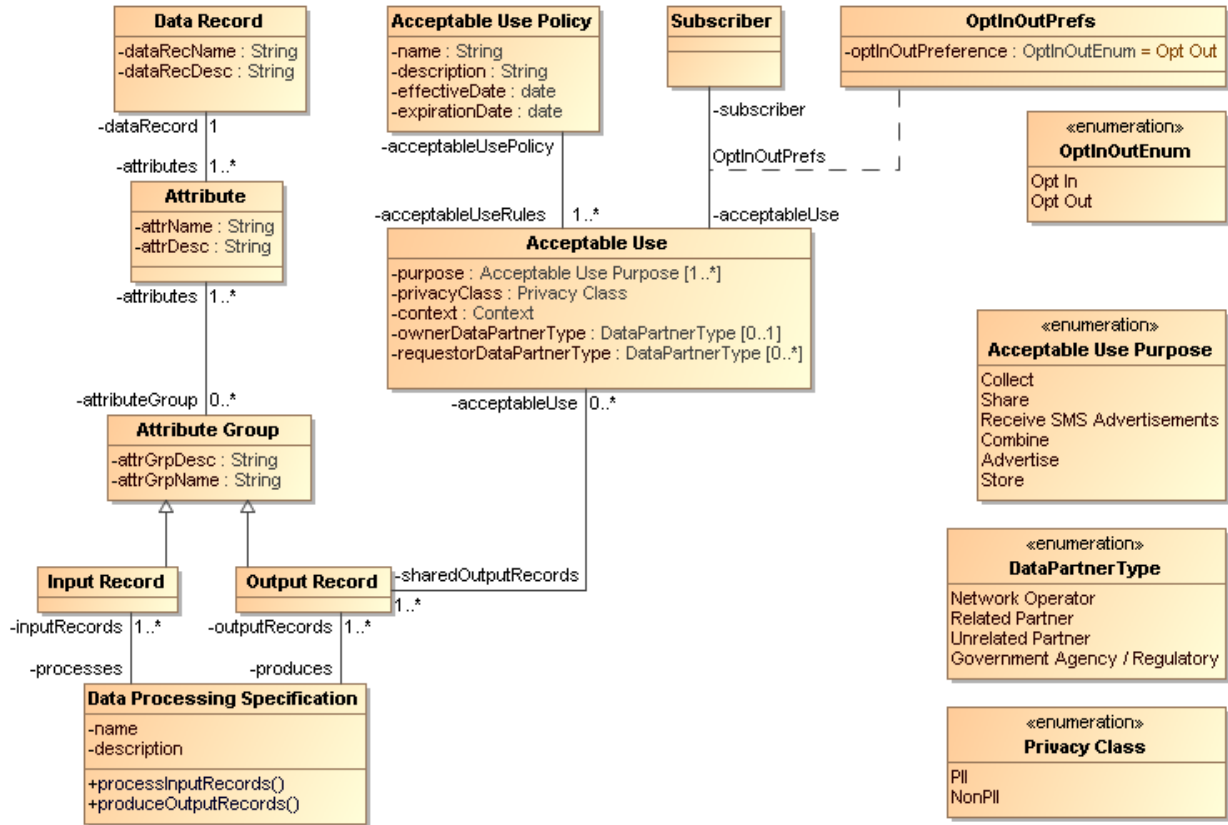


Figure 3: Meta-Model Data Diagram

Table 1: Meta-Model Concepts Terminology

Name	Description	Attributes
Acceptable Use	The acceptable use policy, as defined by the data owner, defines the acceptable use associated with a subscriber's opt-in preferences. Opt-in preferences associated with the data owner's legal, regulatory, and contractual obligations may be relaxed by subscriber opt-ins to more specific acceptable use rules that include less private data (e.g., PII attributes).	acceptableUsePolicy purpose - The purpose or purposes for which this policy may be used by the data partners across the data value chain. privacyClass context ownerDataPartnerType requestorDataPartnerType subscriber sharedOutputRecords - Attribute groups that are bound to the terms of this acceptable use policy.
Acceptable Use Policy	The acceptable use policy, as defined by the data owner, defines the acceptable use associated with a subscriber's opt-in preferences. Opt-in preferences associated with the data owner's legal, regulatory, and contractual obligations may be relaxed by subscriber opt-ins to more specific acceptable use rules that include less private data (e.g., PII attributes).	name - A descriptive name for the acceptable use policy. description - A description for this acceptable use policy. effectiveDate - The begin date when the acceptable use policy is effective. expirationDate - The date on which this acceptable use policy is invalid acceptableUseRules
Attribute	The metadata definition of an attribute.	attrName attrDesc attributeGroup dataRecord
Attribute Group	The metadata definition for a grouping of attributes.	attrGrpDesc attrGrpName attributes
Data Processing Specification	A data processing specification defines how one or more input records are processed to produce one or more output records. The data processing specification is defined by a business entity.	outputRecords - The output records associated with this data processing specification. inputRecords - The input records associated with this data processing specification. name - The name of this data processing specification. defines description - A description of this data processing specification.
Data Record	Defines a collection of related attributes.	dataRecName dataRecDesc attributes
Input Record	An attribute group defined for input records. One or more input records may be processed per a data processing specification to produce one or more output records.	processes

ATIS-I-0000043

Name	Description	Attributes
Output Record	An attribute group that defines an output record as a result of one or more input records and a data processing specification.	produces acceptableUse
Subscriber	A customer who subscribes to the network operators wireless service.	acceptableUse NA

Table 2: Meta-Model Concept Enumerations

Name	Description	Enumeration Literals
Acceptable Use Purpose	NA	Collect Share Receive SMS Advertisements Combine Advertise Store
DataPartnerType	NA	Network Operator Related Partner Unrelated Partner Government Agency / Regulatory
OptInOutEnum	Enumerates the opt-in preference setting.	Opt In - Allow is synonymous with opt-in. A subscriber is allowing a specific privacy preference. Opt Out
Privacy Class	NA	PII NonPII

7.2.2 Retainer Requestor Concepts

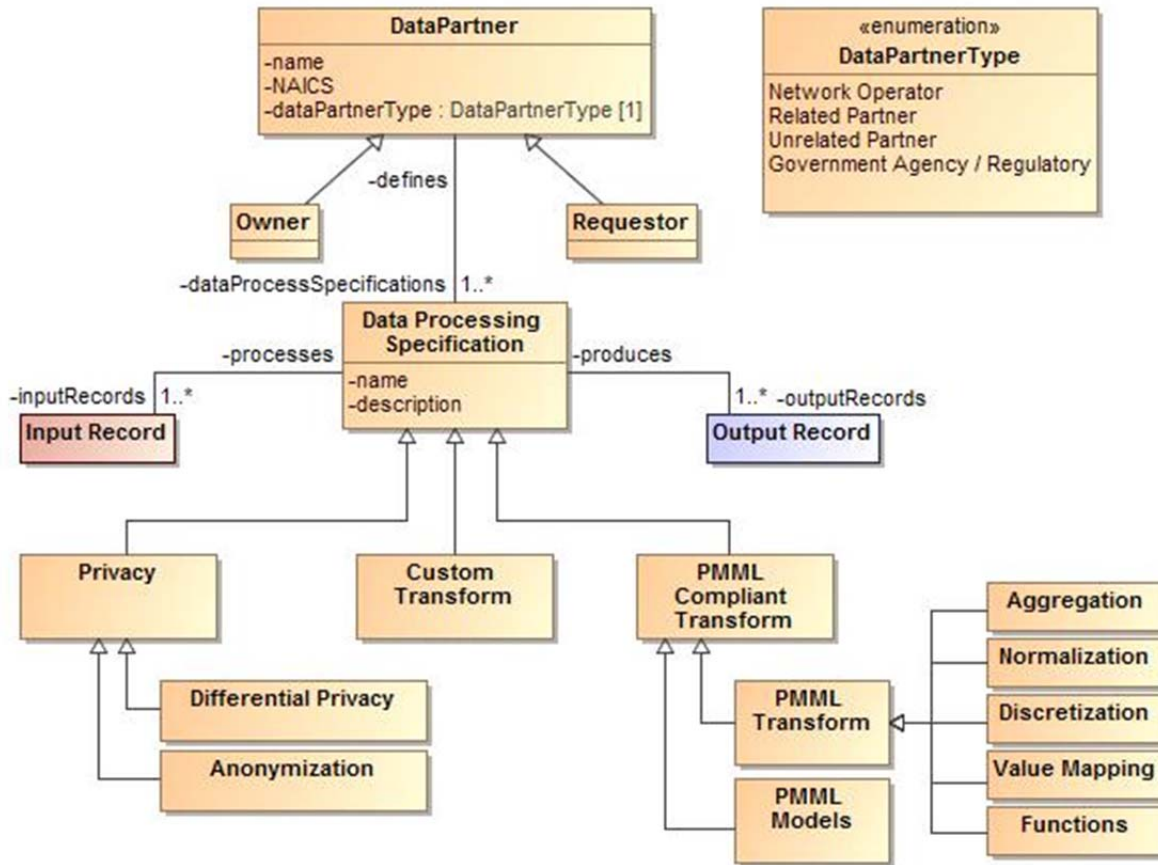


Figure 4: BDA Retainer-Requestor Model

The owner-requestor class diagram defines the general owner-requestor model concepts within a data value chain. Owners and requestors are data partners. Owners and requestors maintain their own data processing specification(s) describing transformations of one or more input records to one or more output records. A data processing specification describes how data is processed from input records to yield output records. This model allows for the specification of very simple or very complex data flows because output record(s) of one process can be used as input record(s) to another data processing specification. Data processing specifications may take on many forms, but the most important concept is that they are associated with well-known concepts and that they have input and output records associated with them. Customized transforms may be defined as well as some well-known transformations such as Predictive Modeling Markup Language (PMML) compliant and differential privacy and anonymization techniques.

Table 3: BDA Retainer-Requestor Terminology

Name	Description	Attributes
Aggregation	Data summarization along one or more dimensions for a continuous attribute (e.g., counts, sum, averages, etc.).	
Anonymization	NA	

ATIS-I-0000043

Name	Description	Attributes
Custom Transform	Any owner defined custom data processing.	
Data Processing Specification	A data processing specification defines how one or more input records are processed to produce one or more output records. The data processing specification is defined by a business entity.	outputRecords - The output records associated with this data processing specification. inputRecords - The input records associated with this data processing specification. name - The name of this data processing specification. defines description - A description of this data processing specification.
DataPartner	The business entity in the owner requestor model.	name - The name of the business entity. NAICS dataProcessSpecifications dataPartnerType
Differential Privacy	Differential privacy techniques seek to prevent re-identification of individuals in aggregate data while preserving the utility of the set. Differential privacy is defined in terms of release of the data as opposed to the data set itself. Differential privacy techniques range may be static or dynamic. A static example would be introducing noise into a data-set (Laplace Transforms). Dynamic techniques are mainly concerned with sequential queries on a data set.	
Discretization	The converting of continuous attributes into discrete values such as nominal attributes or ranges (e.g., binning).	
Functions	Applying a function to one or more attributes to derive a new attribute.	
Input Record	An attribute group defined for input records. One or more input records may be processed per a data processing specification to produce one or more output records.	processes
Normalization	Normalization is the mapping input values to a specific range of values.	
Output Record	An attribute group that defines an output record as a result of one or more input records and a data processing specification.	produces acceptableUse
Retainer	The business entity playing the role of the data owner of data records in the context of a data exchange interaction with another business entity (requestor) in the data value chain.	
PMML Compliant Transform	Any type of data processing within the predictive modeling markup language purview.	

Name	Description	Attributes
PMML Models	Models supported by PMML: association rules, sequences, classification, regression, clustering, time series, and mixed models.	
PMML Transform	A data transformation supported by PMML.	
Privacy	Privacy related data processing. This may range from any number of privacy related functions such as: anonymization, transforming via differential privacy techniques, etc.	
Requestor	The business entity playing the role of a requestor of shared data in the context of a data exchange interaction with another business entity (owner) in the data value chain.	
Value Mapping	Simply mapping discrete values to discrete values.	

Table 4: BDA Retainer-Requestor Concept Enumerations

Name	Description	Enumeration Literals
DataPartnerType	The role that the data partner plays within the value chain, irrespective of the owner/requestor role.	<p>Network Operator</p> <p>Related Partner</p> <p>Unrelated Partner</p> <p>Government Agency / Regulatory</p>

7.2.2.1 Retainer/Requestor Shareable Data Records List Messages

The owner/requestor model provides messaging services for:

- Requestors to request a list of shared records; and
- Owners to respond with a list of records available for sharing.

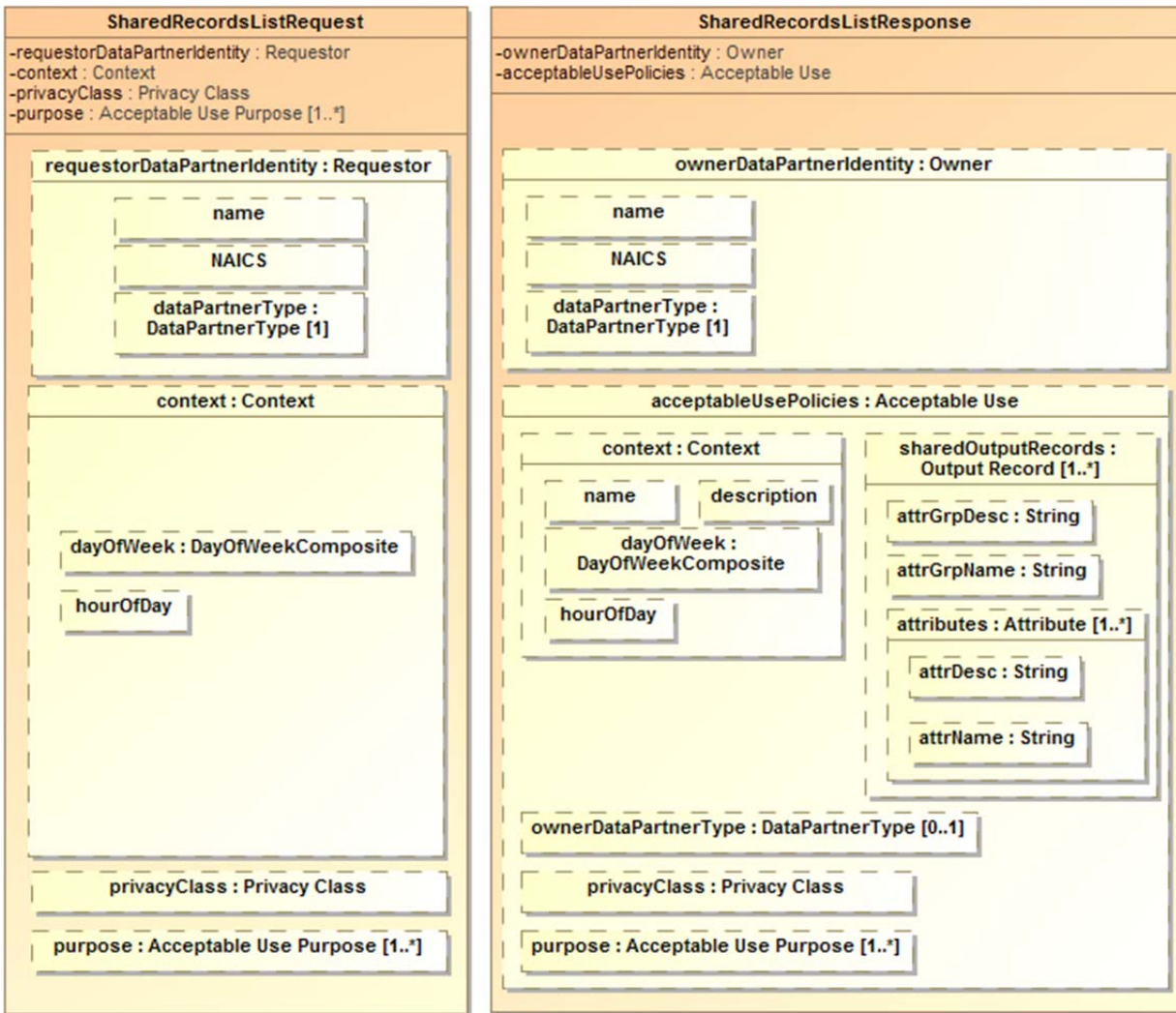


Figure 5: Retainer-Requestor Shareable Data Record List Messages

Name	Description	Attributes
SharedRecordsListRequest		requestorDataPartnerIdentity context privacyClass purpose
SharedRecordsListResponse		ownerDataPartnerIdentity acceptableUsePolicies

7.2.2.2 Retainer/Requestor Data Sharing Messages

The owner/requestor model provides messaging services for:

- Requestors to request the underlying data based on a sharable records list from the owner; and
- Owners to respond with the actual shared data and metadata associated with the data.

7.2.3 Context (Jurisdiction, Locations, Date/Time)

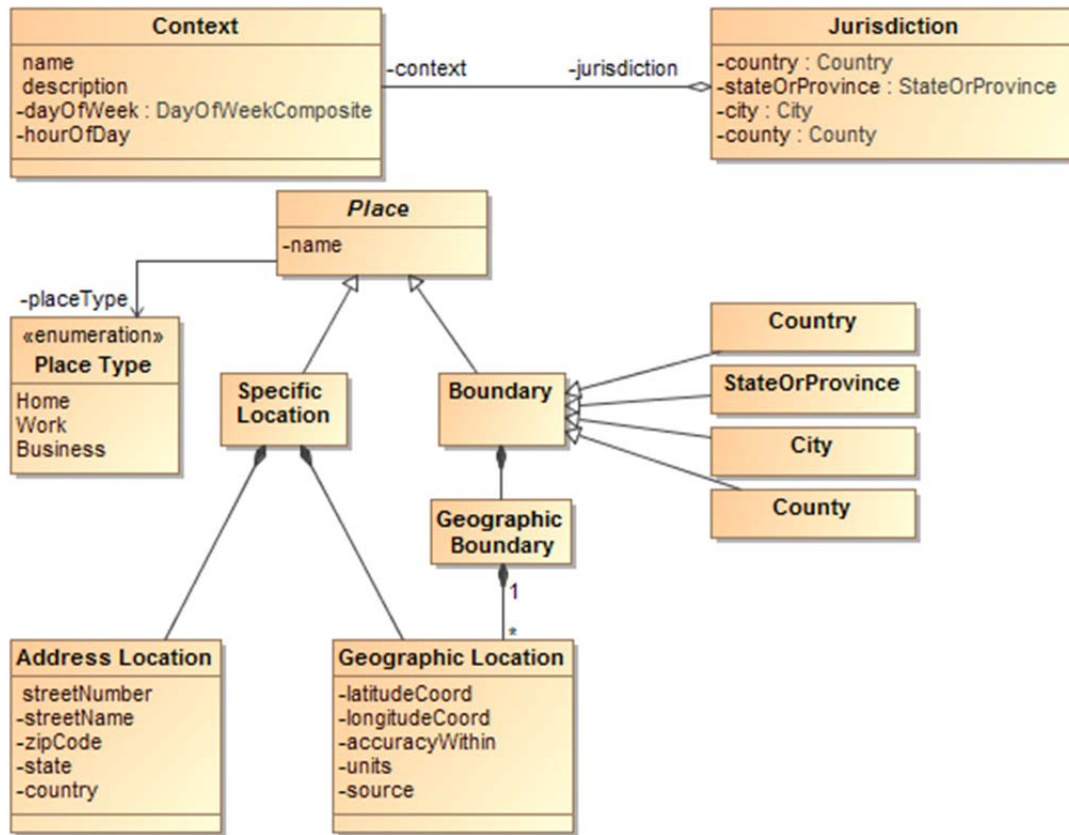


Figure 6: Context Definition Concepts

Table 5: Context Aware Terminology

Name	Description	Attributes
Address Location	The location of a place given by the street address, state, zipcode, and country.	streetNumber streetName zipCode state country NA
Boundary	An generic representation of a boundary.	NA
City	A city is a place that can be associated to a specific point or center of a boundary or a boundary.	
Context	Defines the various parameters to allow for context-aware data sharing, e.g., jurisdiction.	name description dayOfWeek hourOfDay jurisdiction

ATIS-I-0000043

Name	Description	Attributes
Country	A place that represents a country or a boundary associated with a country.	
County	A place that represents a specific county location as a geographic point (e.g., lat/long) or geographic boundary on a map.	
Geographic Boundary	A boundary defined by three or more geographic locations.	
Geographic Location	A geographic location of a specific point location given by a latitude/ longitude coordinate.	latitudeCoord - The latitude coordinate for a geographic location. longitudeCoord - The longitude coordinate for a geographic location. accuracyWithin units source
Jurisdiction	The jurisdiction within which a business entity must comply with privacy laws and regulations.	country stateOrProvince city county context
Place	An name of a place that can be represented by either a specific point, a boundary, or a logical place.	name placeType
Specific Location	A location specific to a point on a map (e.g., not the opposite of a boundary location).	
StateOrProvince	A place that represents a specific state or province location as a geographic point (e.g., lat/long) or geographic boundary on a map.	

Table 6: Context Enumerations

Name	Description	Enumeration Literals
Place Type	Common types of locations.	Home Work Business

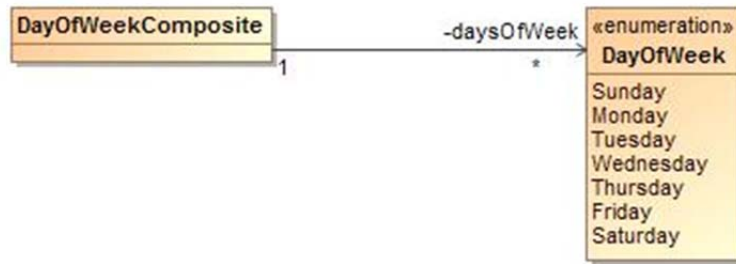






Figure 7: Time Context Date of the Week

7.3 Participants (Actors/Roles/Organization)

Table 7: Data Partner Organizations

Name	Description
 Aggregator[Participant]	An aggregator combines data from various sources to normalize the data into one data set. They typically enrich the source data with reference data, analyze the underlying patterns in big data to produce meaningful results, and package the data for monetization while maintaining privacy of the data set.
 Customer[Participant]	A customer is often referred to as a subscriber in mobile telecommunications. Typically there are multiple users associated with one customer's account. Users on the customer account influence the actual person known as the customer (e.g., subscriber).
 Network Operator[Participant]	A network operator provides voice and data communications services to their customers.
 Product Company[Participant]	A product company produces products (e.g., mobile game apps).

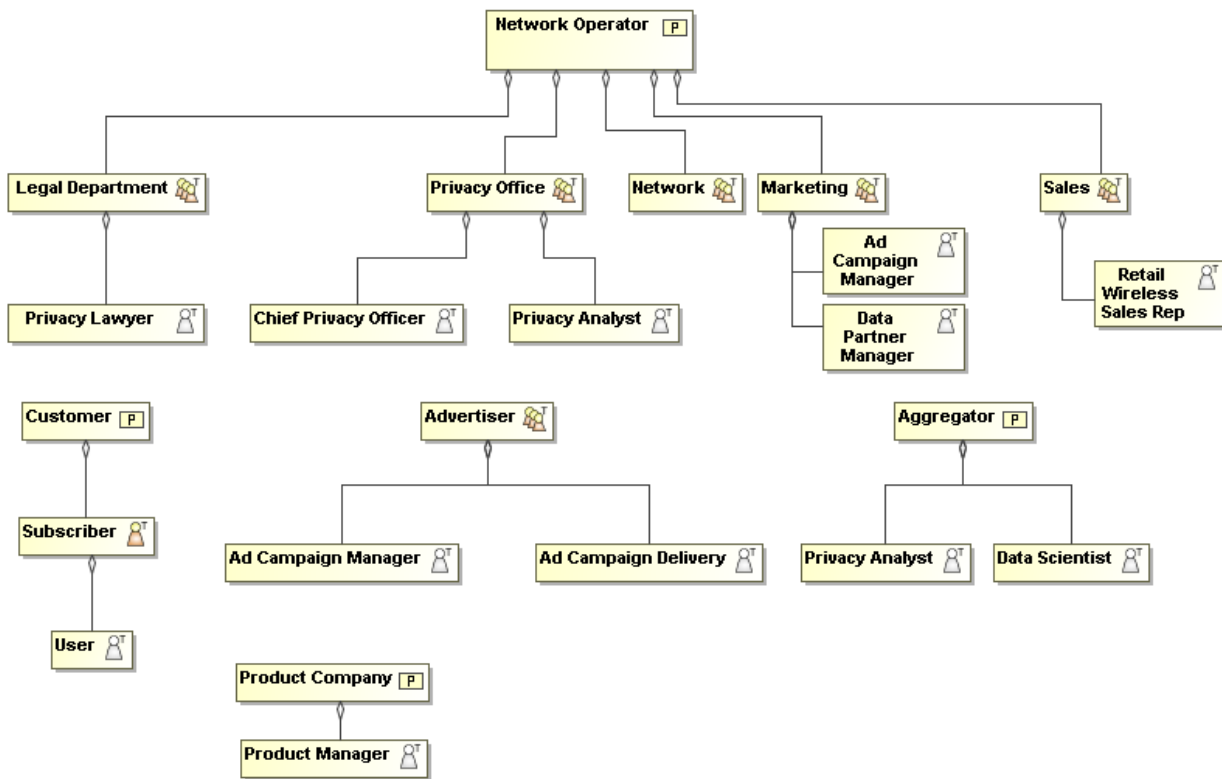





















Figure 8: Typical Participant Organizational Roles

Table 8: Typical Participant Organizational Role Descriptions

Name	Description
 Advertiser[Organization]	An advertising company may act as a related third party requestor. They will request data sharing and advertising services from a network operator in order to more appropriately target and deliver advertisements to mobile customers.
 Network[Organization]	The organization, within the network operator, responsible for building and maintaining the underlying network technologies requires delivering voice and data communications services.
 Legal Department[Organization]	The organization, within the network operator, responsible for ensuring compliance with the laws and regulations of those jurisdictions in which it operates.
 Marketing[Organization]	The organization, within the network operator, responsible for acquiring and retaining customers through a differentiated suite of products and services.
 Sales[Organization]	The network operator's sales department.
 Privacy Office[Organization]	Responsible for safeguarding the privacy of individual customers.
 Chief Privacy Officer[Post]	Ultimately responsible for a data owner's privacy policy, working with the legal counsel, internal privacy analysts, and other departments to ensure that privacy and security are maintained at an appropriate level to satisfy the legal and regulatory requirements within the company's operating jurisdictions.
 Privacy Lawyer[Post]	The legal counsel for any data partner ensures that privacy laws and regulations are understood and implemented by the data partner's privacy office.
 Privacy Analyst[Post]	A network operator's privacy analyst must understand the privacy domain from a business and technical perspective. This person is responsible for populating the metadata model with the appropriate content that constrains data sharing at an appropriate level to satisfy the legal and regulatory requirements while preserving data utility and the monetization requirements of the business.
 Ad Campaign Manager[Post]	A third party data partner may have a campaign manager responsible for managing advertising campaigns with a network operator. In this case, the ad campaign manager's role is a requestor. They will request data sharing for the purposes of advertising and typically a network technology on which to deliver the advertising content (e.g., SMS, MMS, Notifications).
 Subscriber[Person]	A subscriber is a person or entity who purchases services from a network operator and who is financially responsible for the account. The term subscriber is often used to mean a mobile device user and/or account holder of a network operator. However, a subscriber may or may not be a user of a mobile device if they are simply fulfilling an administrative role on the account.
 Privacy Analyst[Post]	As a requestor in the owner-requestor model, a data aggregator's privacy analyst must protect the interests of the data owner and the individual subscribers as defined in the metadata exchanged among data partners. They must understand the privacy domain from a business and technical perspective. This person is responsible for populating the metadata model with the appropriate content that constrains data sharing at an appropriate level to satisfy the legal and regulatory requirements while preserving data utility and the monetization requirements of the business.
 User[Post]	The end user of a device. The end user may be the subscriber or they may not have any financial responsibility for the account (e.g., an employee using a mobile device paid for by their employer or child on a parent's family plan).

Name	Description
 Ad Campaign Delivery[Post]	A advertiser data partner may have an ad campaign delivery manager responsible for managing, verifying delivery, and measuring the effectiveness of advertising campaigns with a network operator. In this case, the ad campaign manager's role is a requestor. They will request data sharing for the purposes of advertising and typically a network technology on which to deliver the advertising content (e.g., SMS, MMS, Notifications).
 Product Manager[Post]	A product manager is responsible for a product within a company who may provide a product (e.g., a mobile game app).
 Data Scientist[Post]	A data scientist is responsible for creating value out of raw data from the network operator and reference data from data partners. They may work for any of the participant types in this model. They typically possess a comprehensive skill set in the areas of statistical analysis, predictive algorithms, and machine learning, and more broadly, computer science and mathematics.
 Ad Campaign Manager[Post]	A network operator's campaign manager is responsible for managing internal advertising campaigns. They may also provide network operator based advertising services an associated advertising data partner (e.g., SMS based advertising campaigns).
 Data Partner Manager[Post]	A network operator's data partner manager is responsible for managing related partners (e.g., aggregators, advertising companies, product companies, etc.). They should also have knowledge of their unrelated partners who may be doing business with the network operator's related partners.
 Retail Wireless Sales Rep[Post]	The network operator's sales representative for the wireless voice and data communications services and mobile devices (e.g., handsets).

7.4 Participant Data Models

This section defines the typical, and relevant, data models for the participants identified in the use cases. The participant's data model defines the data records and attributes that they typically use to run their business including collection, storage, processing, and storing derived data records.

7.4.1 Network Operator Data Model

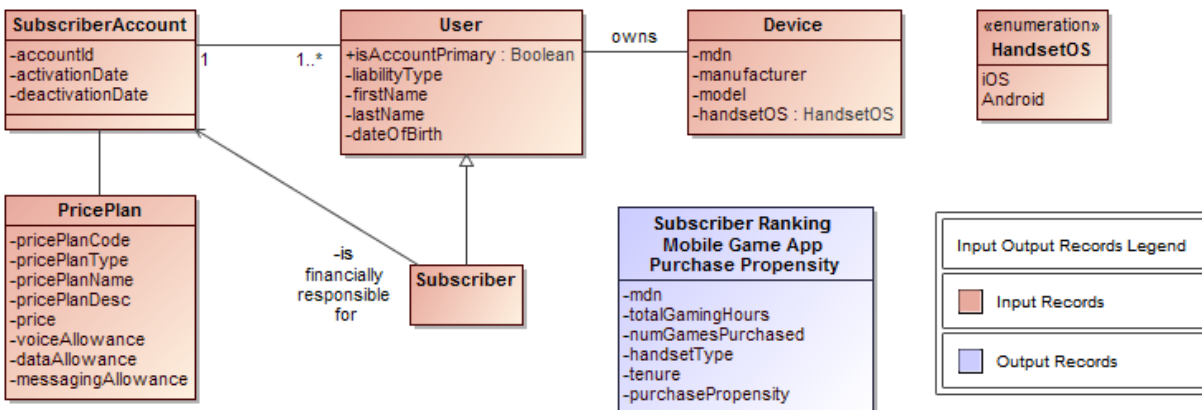


Figure 9: Typical Network Operator Data Model

ATIS-I-0000043

The above shows a typical participant data model for a Network Operator and the data records typically stored to for subscriber management: subscriber account, price plan, individual users on the account, device, and an output record (e.g., mobile game app purchase propensities) to be shared in the Mobile Game App example use case.

Table 9: Network Operator Data Model Terminology

Name	Description	Attributes
Device	The user's mobile device characteristics.	mdn manufacturer model handsetOS
PricePlan	The subscriber's price plan associated with the bundle of services delivered by the network operator.	pricePlanCode pricePlanType pricePlanName pricePlanDesc price voiceAllowance dataAllowance messagingAllowance
Subscriber	A customer who subscribes to the network operators wireless service.	acceptableUse
Subscriber Ranking Mobile Game App Purchase Propensity	An example of a shared data record for the mobile game app company SMS advertising use case. Defines a shareable data record to store the results of a subscriber's propensity to purchase mobile game apps.	mdn totalGamingHours numGamesPurchased handsetType tenure purchasePropensity
SubscriberAccount	The subscriber's account information. Typically contains PII for the purposes of billing, sending advertisements, and sharing non-PII and PII data per subscriber's opt-in settings.	accountId activationDate deactivationDate
User	The end user of a device. The end user may be the subscriber or they may not have any financial responsibility for the account (e.g., an employee using a mobile device paid for by their employer or child on a parent's family plan).	isAccountPrimary liabilityType firstName lastName dateOfBirth

7.4.2 Mobile Gaming App Company Data Model

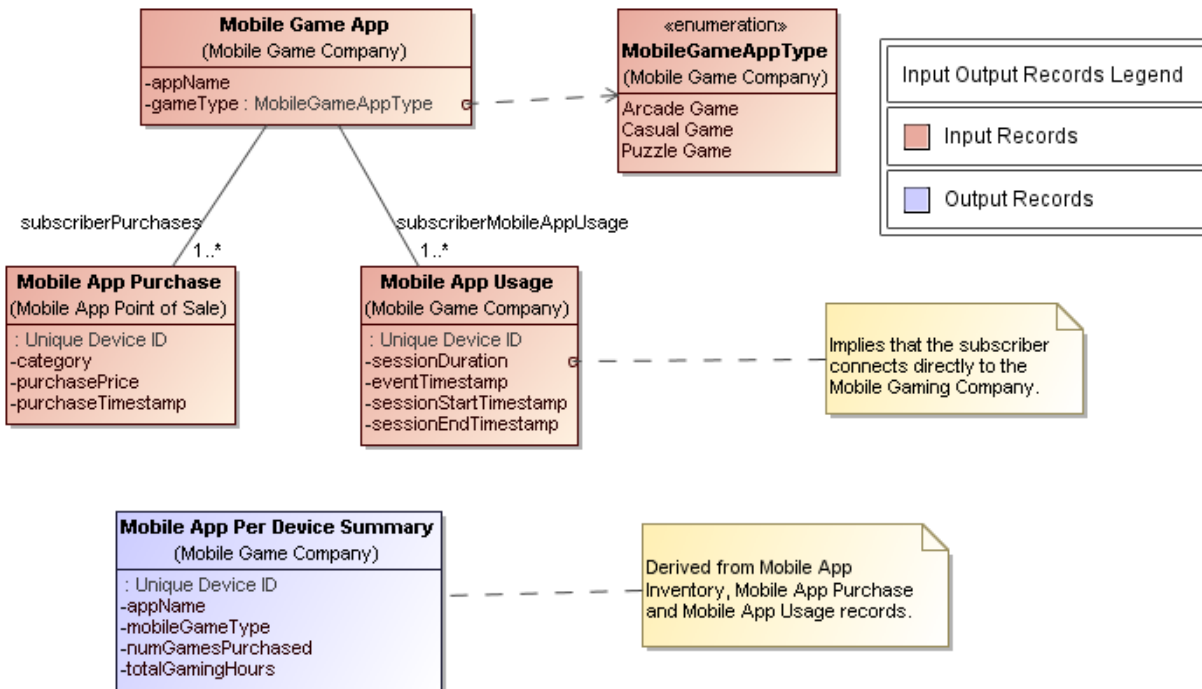


Figure 10: Typical Mobile Gaming Company Data Model

The Mobile Gaming App Company data model shows the relevant mobile app purchase history, mobile app usage collected by the mobile gaming company, and an output data record to be shared with the network operator (e.g., Mobile App Per Device Summary).

Name	Description	Attributes
Mobile App Per Device Summary	A summarization of mobile app usage per unique device. This record is intended to be shared.	appName mobileGameType numGamesPurchased - The number of games purchased. totalGamingHours - The total number of hours spent playing games.
Mobile App Purchase	An audit trail of mobile app purchases per unique device or subscriber.	category purchasePrice purchaseTimestamp - The date and time of purchase.
Mobile App Usage	Per subscriber mobile game usage measurements.	sessionDuration eventTimestamp sessionStartTimestamp sessionEndTimestamp
Mobile Game App	Represents the mobile game application installed and/or owned by the subscriber.	appName NA NA gameType

Name	Description	Enumeration Literals
MobileGameAppType	NA	Arcade Game Casual Game Puzzle Game

7.4.3 Advertiser Data Model

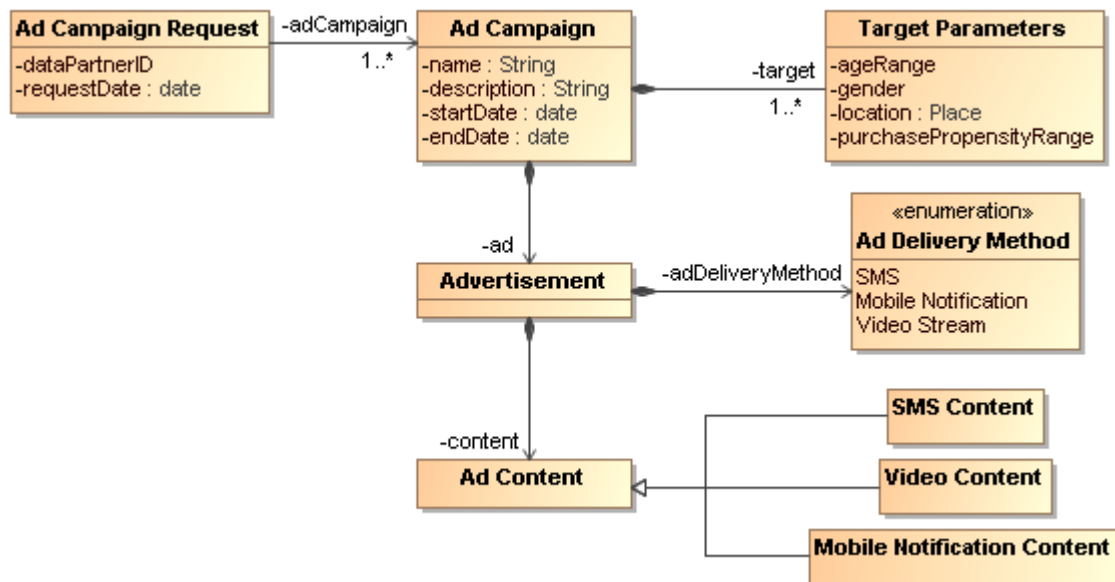


Figure 11: Typical Advertiser Data Model

ATIS-I-0000043

The ad campaign management domain consists of advertising campaign metadata to enable the advertiser to request per-subscriber targeting of ad campaigns based on the targeting parameters and the desired delivery method and content.

Name	Description	Attributes
Ad Campaign	Defines the parameters that describe an advertising campaign including when the campaign should be run, whom the ads should target, and the content of advertisement.	name description startDate endDate target ad
Ad Campaign Request	The parameters sent to the network operator for an advertising campaign targeted to a subscriber.	dataPartnerID requestDate adCampaign
Ad Content	An abstract representation for the content of an advertisement.	
Advertisement	An abstract representation of an advertisement.	adDeliveryMethod content
Mobile Notification Content	The text content of an SMS message without the source and destination telephone numbers.	
SMS Content	The text content of an SMS message without the source and destination telephone numbers.	
Target Parameters	The demographic, geographic, and behavioral targeting parameters to target the delivery of an advertisement.	ageRange gender location NA purchasePropensityRange
Video Content	The streaming video content for a streaming video advertisement.	

Name	Description	Enumeration Literals
Ad Delivery Method	Typically advertisement delivery methods when advertising to a network operator's customers.	SMS Mobile Notification Video Stream

7.4.3.1 Ad Campaign Request Message

The following shows a typically request sent from a related partner to the network operator to request an advertising campaign.

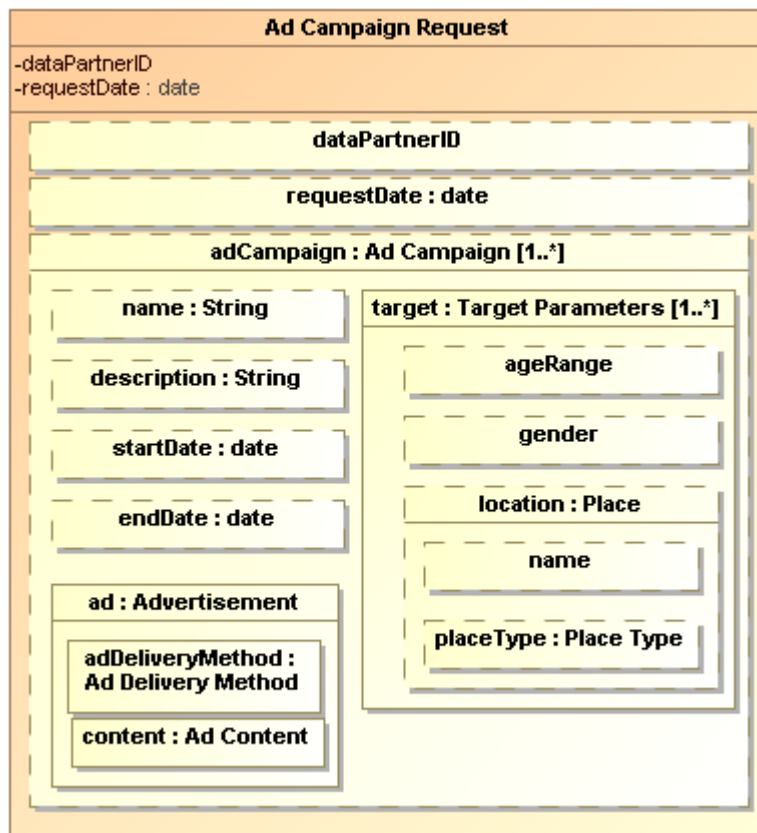


Figure 12: Ad Campaign Request

Table 10: Ad Campaign Request Message Description

Name	Description	Attributes
Ad Campaign Request	The parameters sent to the network operator for an advertising campaign targeted to a subscriber.	dataPartnerID requestDate adCampaign

8 Example Use Cases

Various use cases are provided in this section to illustrate how the metadata model is populated to enable data sharing and advertising services.

8.1 Full PII Sharing: Mobile Gaming Use Case

The Mobile Gaming use case enables data sharing between the network operator and a mobile gaming company, a related partner. The mobile gaming company also has direct relationships with an advertising company and the mobile app point-of-sale provider, both unrelated partners from the network operator's perspective. The data shared in this use case is considered full-PII as the mobile number is shared to provide the mobile gaming company the ability to send SMS advertisements to the mobile device end-user. The mobile device end-user opted-in to SMS advertising when they subscribed to the network operator. As such, the network operator provides the subscriber's mobile number to third parties for the purposes of receiving relevant SMS advertisements. The network operator is then responsible to controlling the use of this information by acting as a proxy to the mobile gaming company for SMS advertisements and according to the acceptable use metadata that is setup for the subscriber at the time of their activation.

8.1.1 Mobile Gaming Use Case: Sharing Request

Figure 13 depicts a request to share the top 1,000 mobile numbers of the customers most likely to buy game apps.

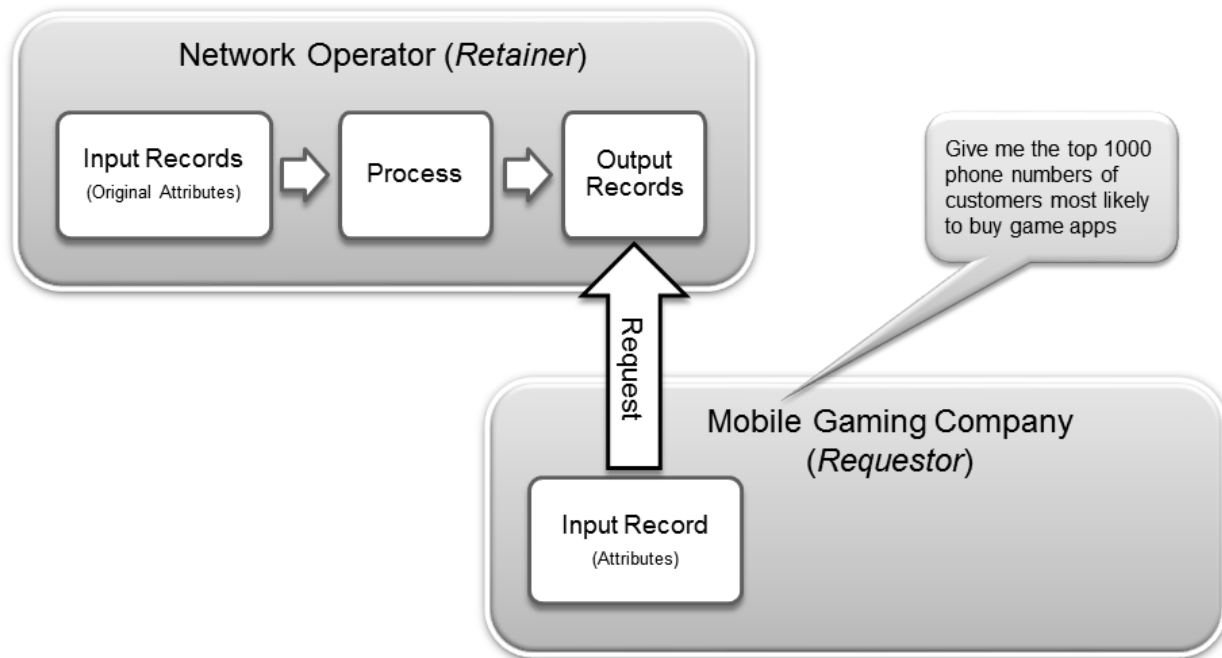


Figure 13: Mobile Gaming Use Case - Sharing Request

8.1.2 Mobile Gaming Use Case: Data Sharing Request Detail

Figure 14 depicts the detail of a PII sharing request from a related partner (e.g., Rovio mobile game app company) to the network operator. The network operator authenticates the requestor; creates a sharing request context, traverses the data lineage as populated (by the network operator) in the data process metadata, and verifies the subscriber specific sharing acceptable use policy (e.g., opt-ins).

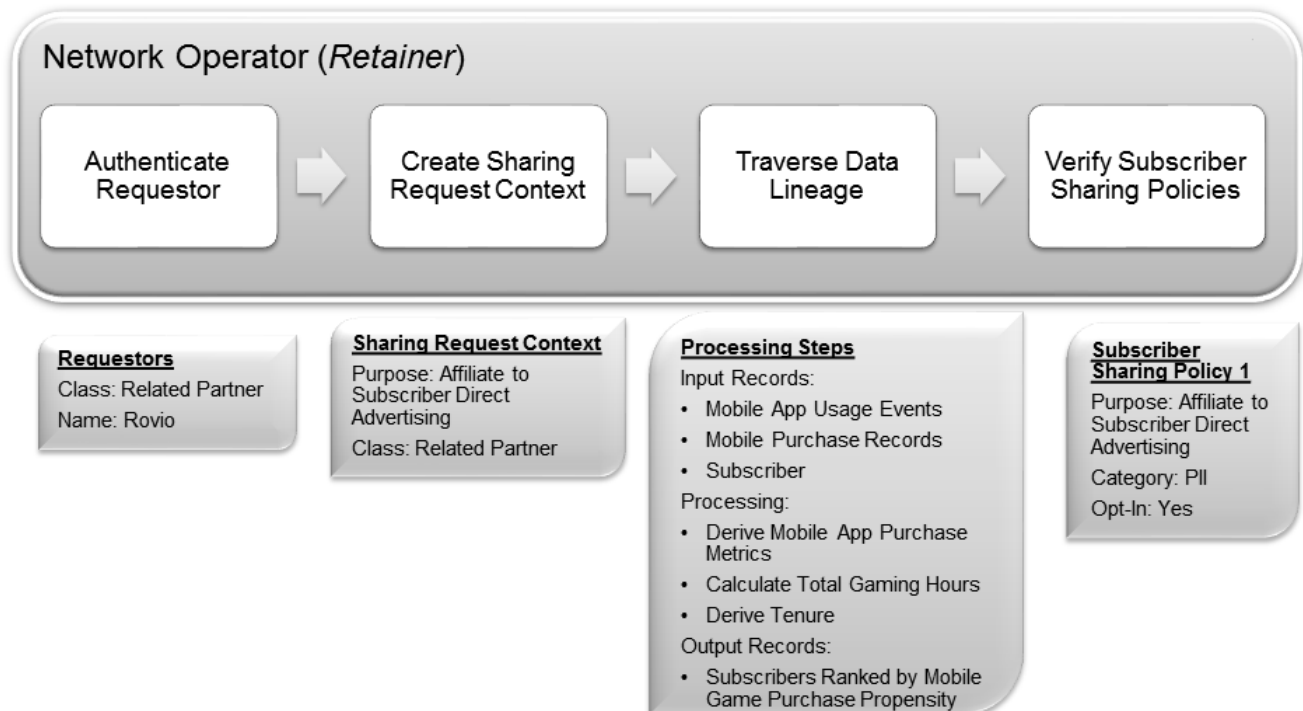


Figure 14: Mobile Gaming Use Case - Data Sharing Request Detail

8.1.3 Mobile Gaming Use Case: Data Processing Detail

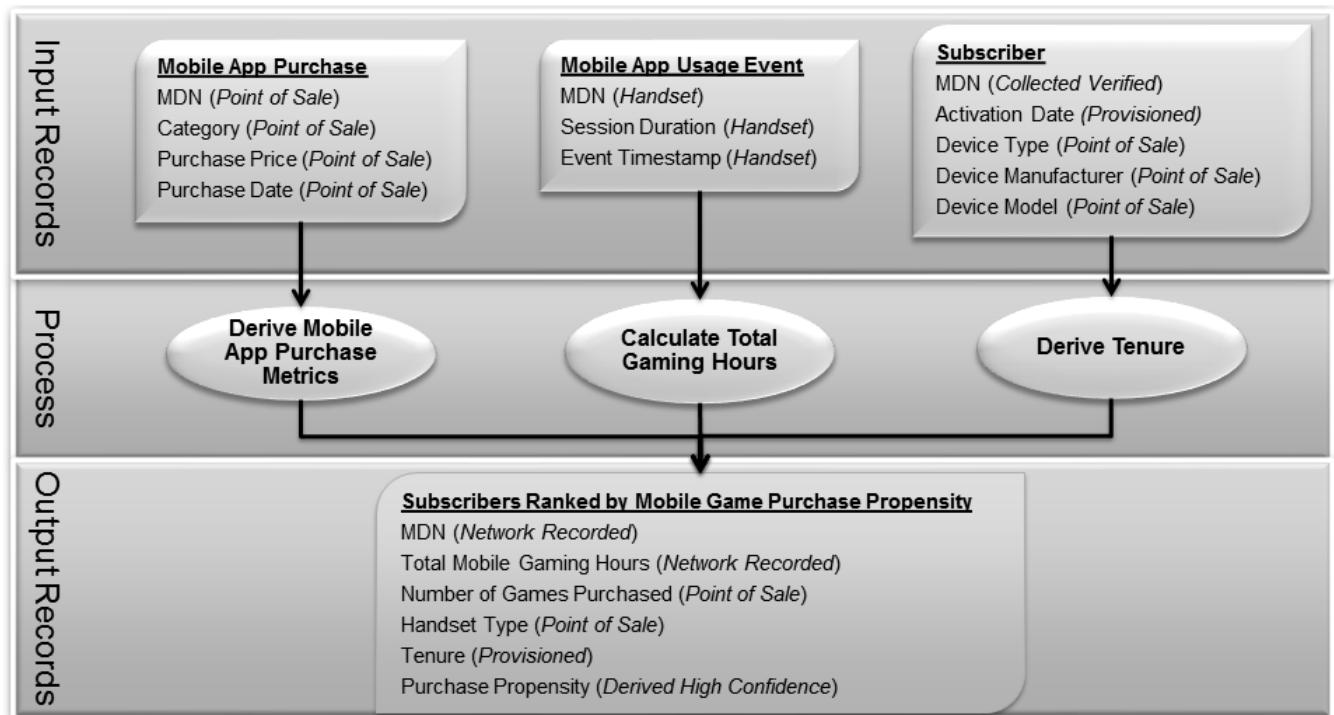


Figure 15: Mobile Gaming Use Case - Data Processing Detail

8.1.4 Mobile Gaming Use Case: Data Sharing Response Detail

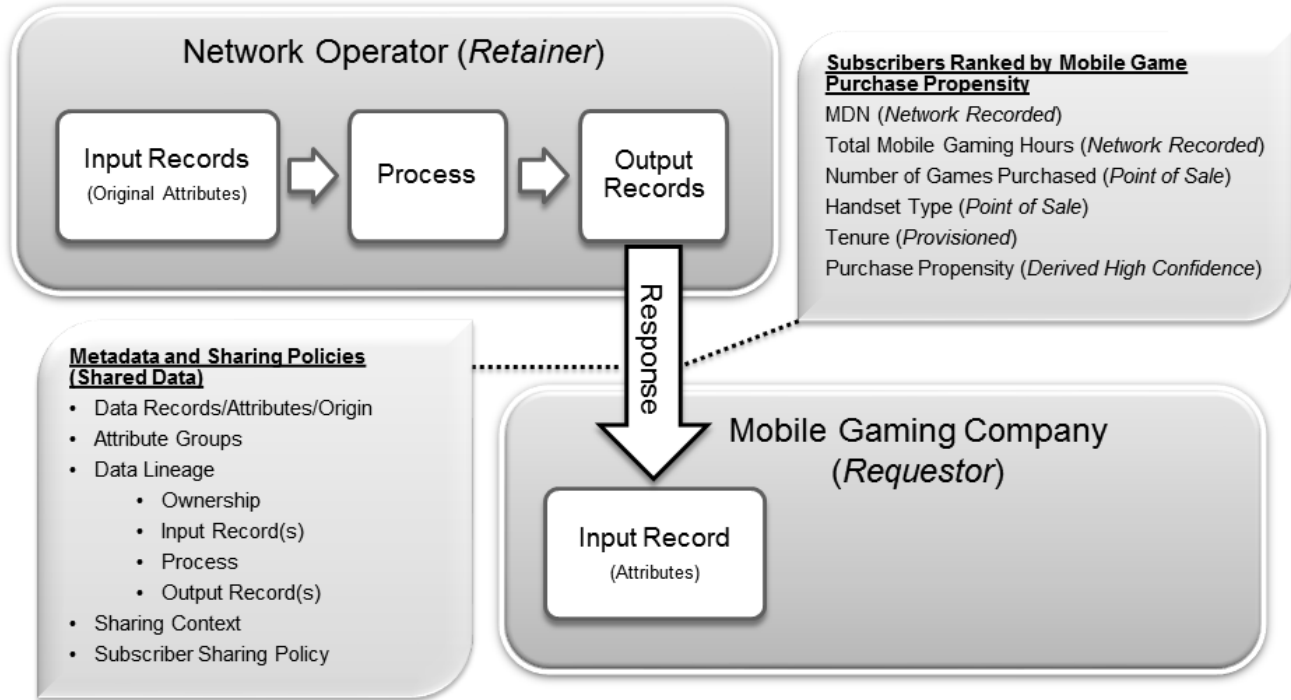


Figure 16: Mobile Gaming Use Case - Data Sharing Response

8.1.5 Mobile Gaming Use Case: SMS Advertisements

Figure 20, Figure 21, and Figure 22 depict the steps that a data requestor takes upon acquisition of the shared data.

1. The mobile gaming company acquires the input records and associated metadata (e.g., subscriber purchase propensity data); verifies acceptable sharing policies; and sends SMS advertisement (action request(s) to network operator.
2. The network operator verifies subscriber opt-in acceptable use in the current data sharing context with the mobile gaming company and sends SMS advertisements to the top 1,000 mobile gamers. This verification step respects the most current acceptable use policy (opt-in/out) settings of the subscriber. For example, when the subscriber opts-out SMS advertising after having previously have opted-in to SMS advertisements.

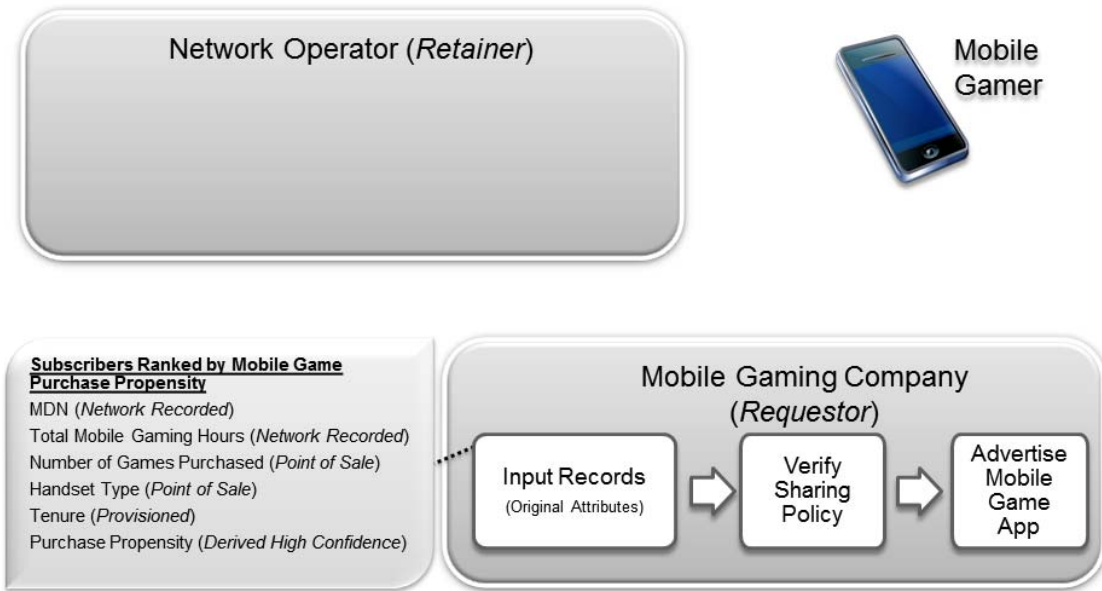


Figure 17: Mobile Gaming Use Case - Advertising to Top Mobile Gamers (Retain Input Records)

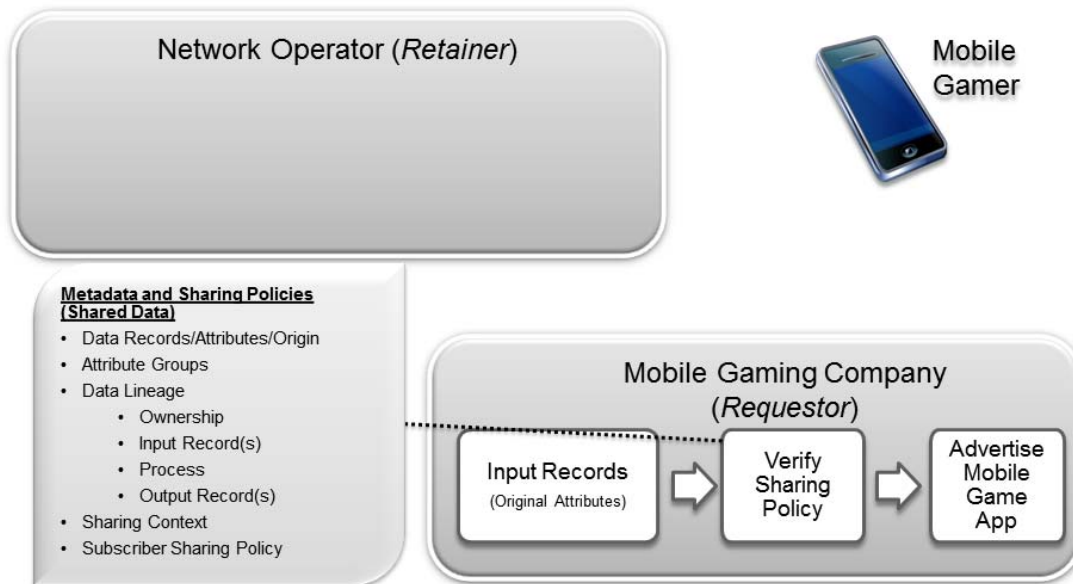


Figure 18: Mobile Gaming Use Case - Requestor Verifies Sharing Policies

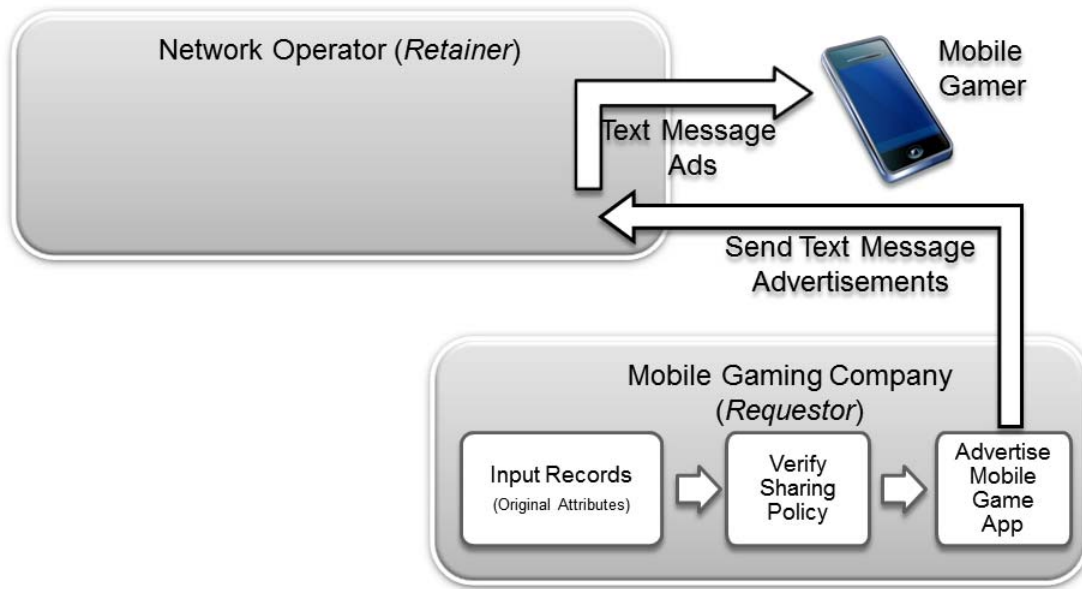


Figure 19: Mobile Gaming Use Case - SMS Advertisements Action Requests/Text Message Ads

8.1.6 Mobile Gaming Use Case: Retainer Metadata Population

This section provides concrete examples of metadata population by the data retainer.

8.1.6.1 Mobile Gaming Use Case: Jurisdictional Context

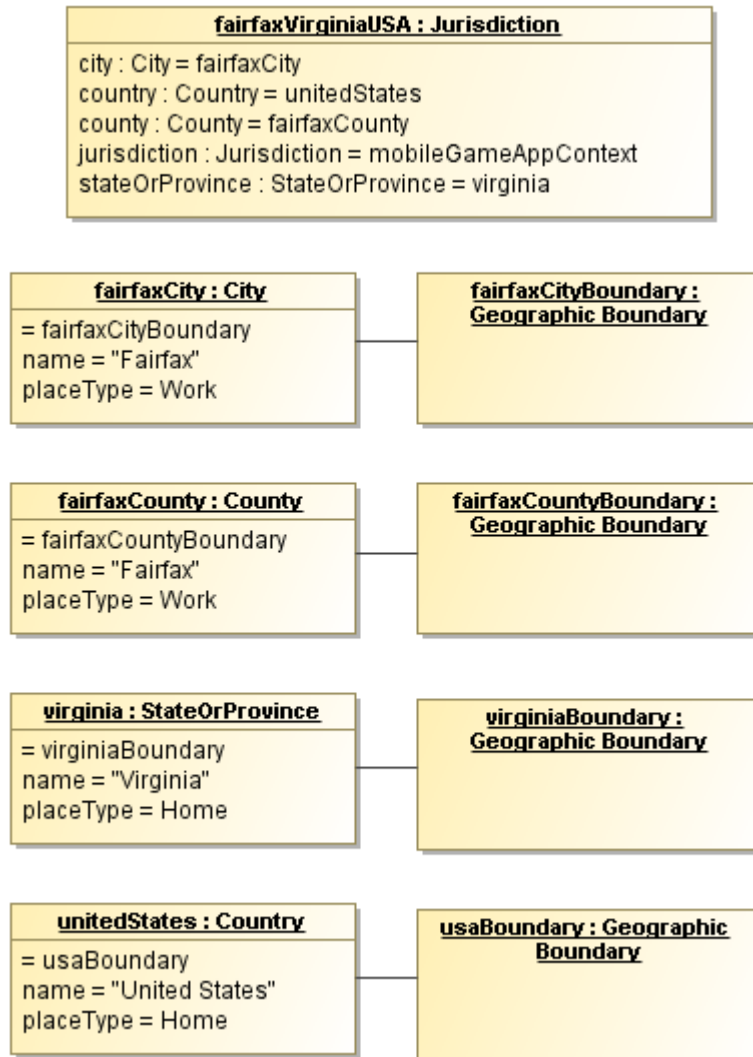


Figure 20: Example Metadata Model Population for Jurisdictional Context

8.1.6.2 Mobile Gaming Use Case: Setup Context & Acceptable Use Policy

Figure 21 shows an example of the setting up the contextual and acceptable use metadata for the Mobile Game App Use Case.

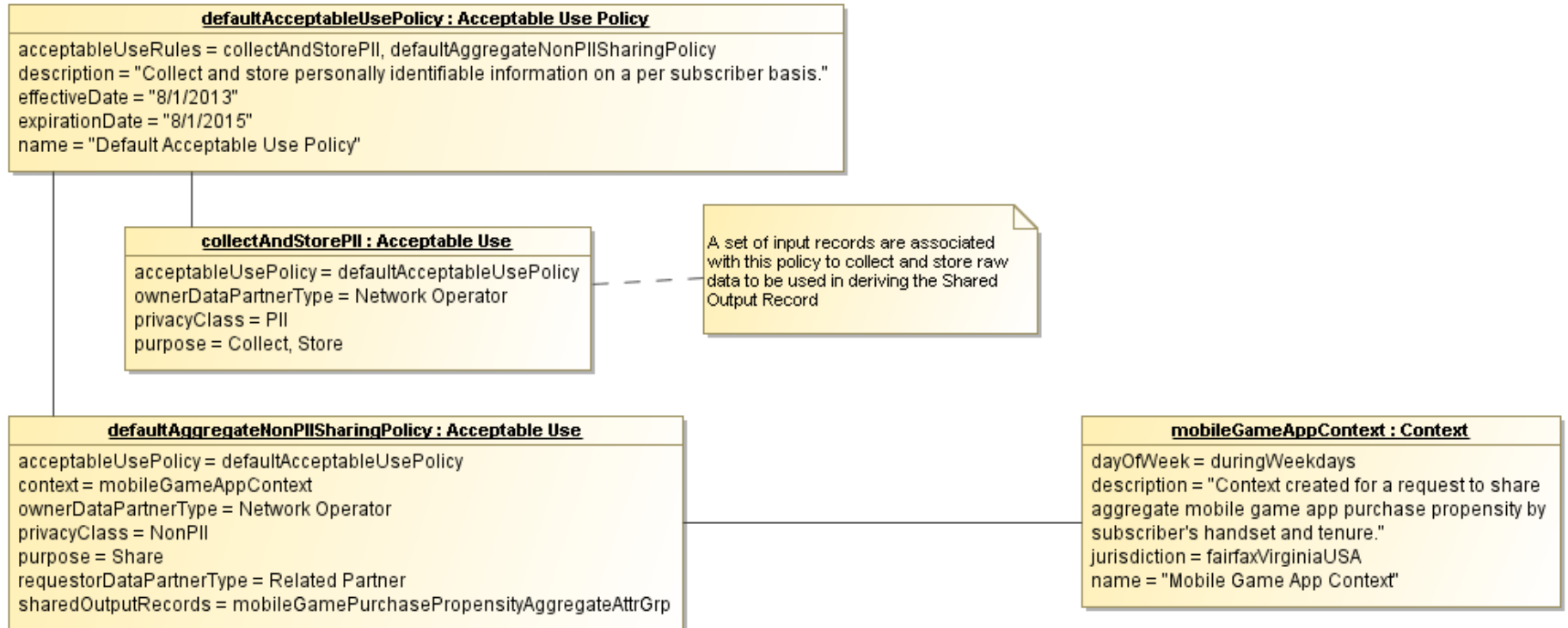


Figure 21: Example Metadata Model Population for Context & Acceptable Use Policy

8.1.6.3 Mobile Gaming Use Case: Setup Data Records, Attributes, & Attribute Groups

Figure 22 shows an example of the setting up the data records, attributes, attribute groups, and output records metadata for the Mobile Game App Use Case.

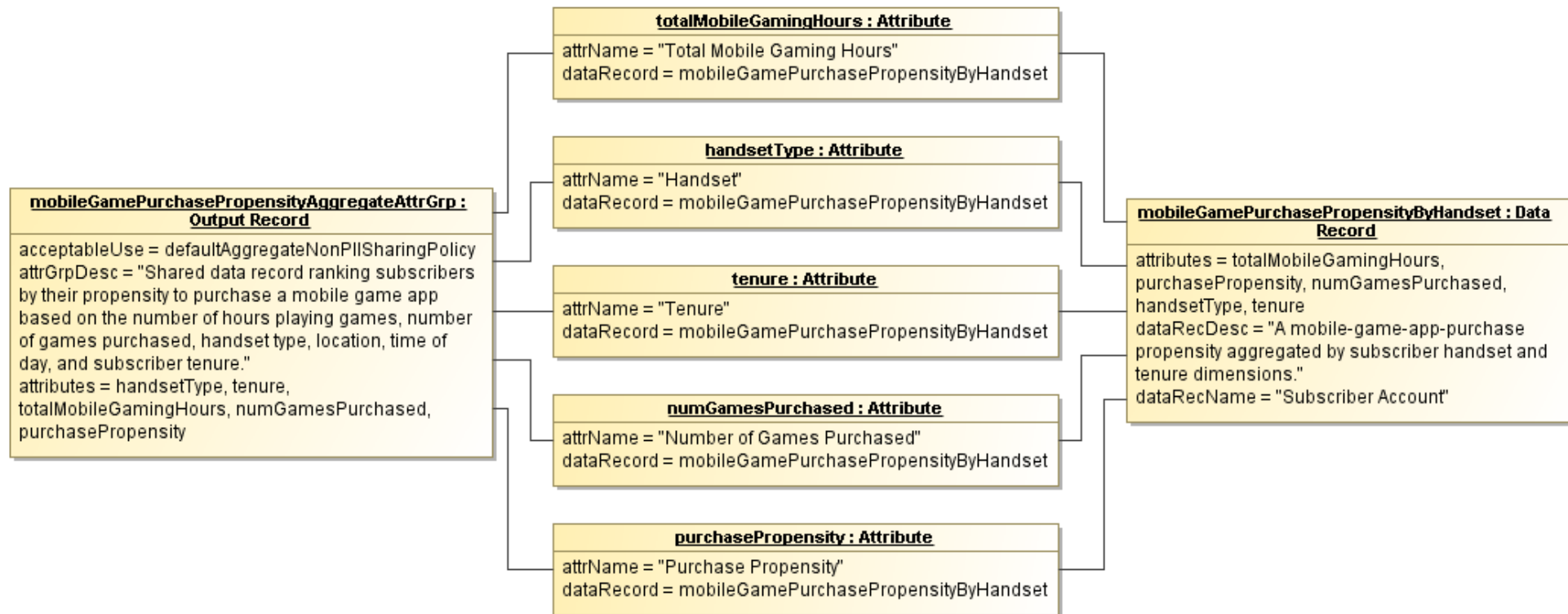


Figure 22: Example Metadata Model Population of Shared Data Records and Attributes

8.1.6.4 Mobile Gaming Use Case: Metadata Populated

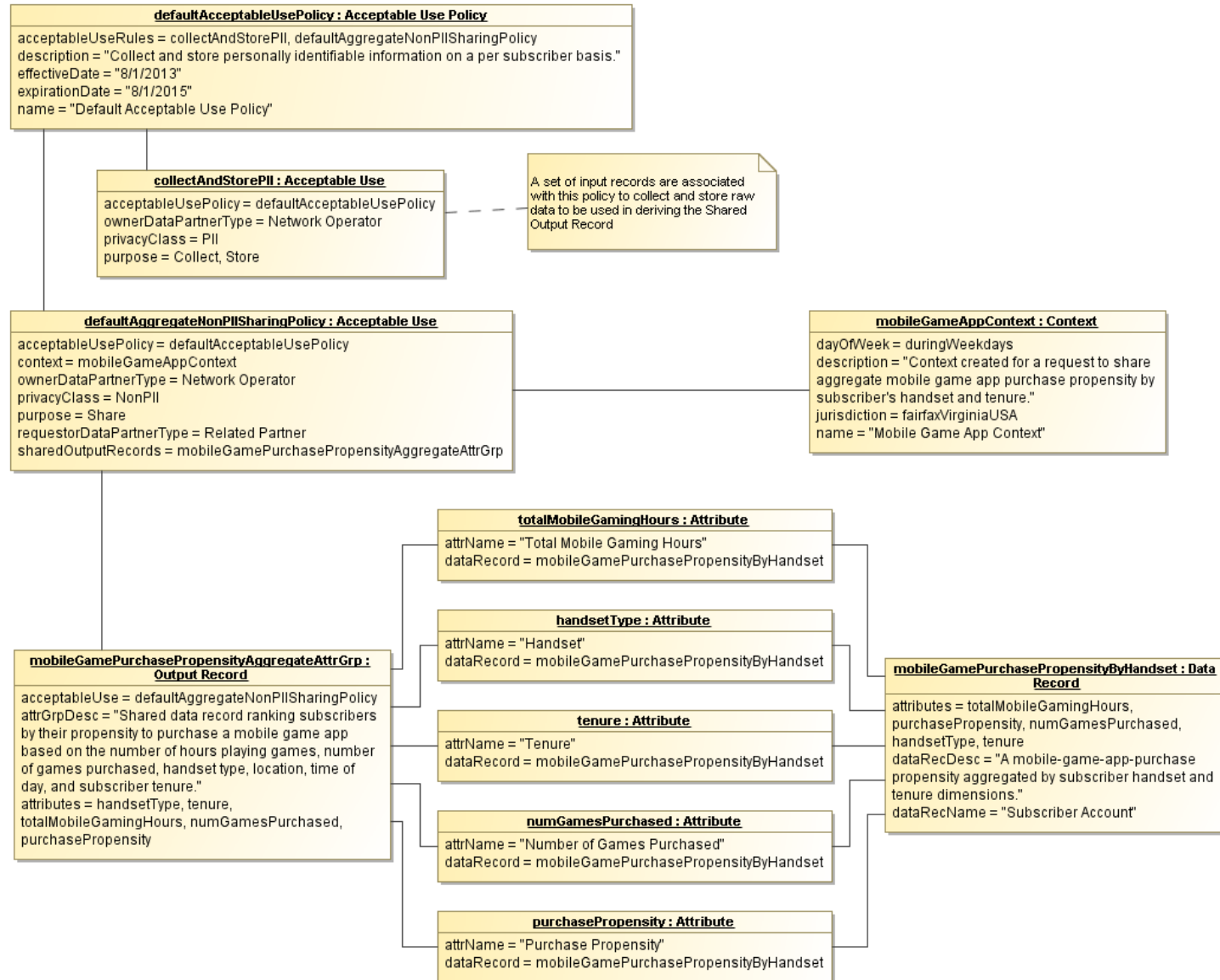


Figure 23: Complete Population of Metadata

8.1.6.5 Mobile Gaming Use Case: Mobile Game Advertisement Metadata

Figure 24 depicts the metadata for a targeted ad campaign delivered via SMS advertisements.

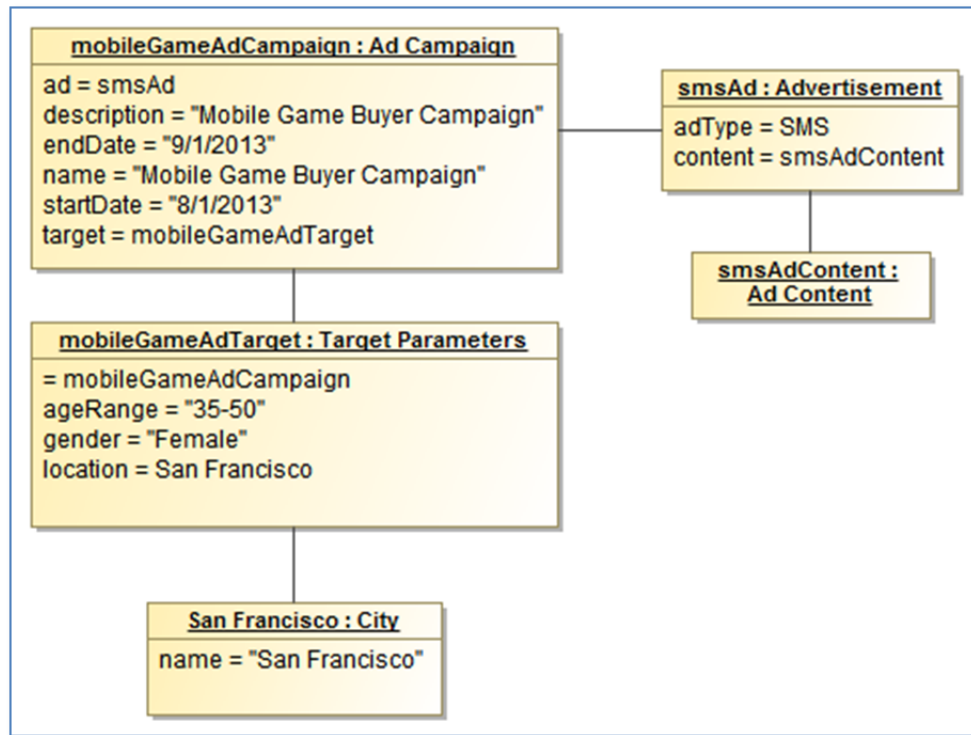


Figure 24: Mobile Game Advertisement

8.2 Limited Sharing: Improving Relevance of Real-Time Ads Use Case

The following diagram the typical interactions among the end-user, network operator, and DSP/DMP-related partner.

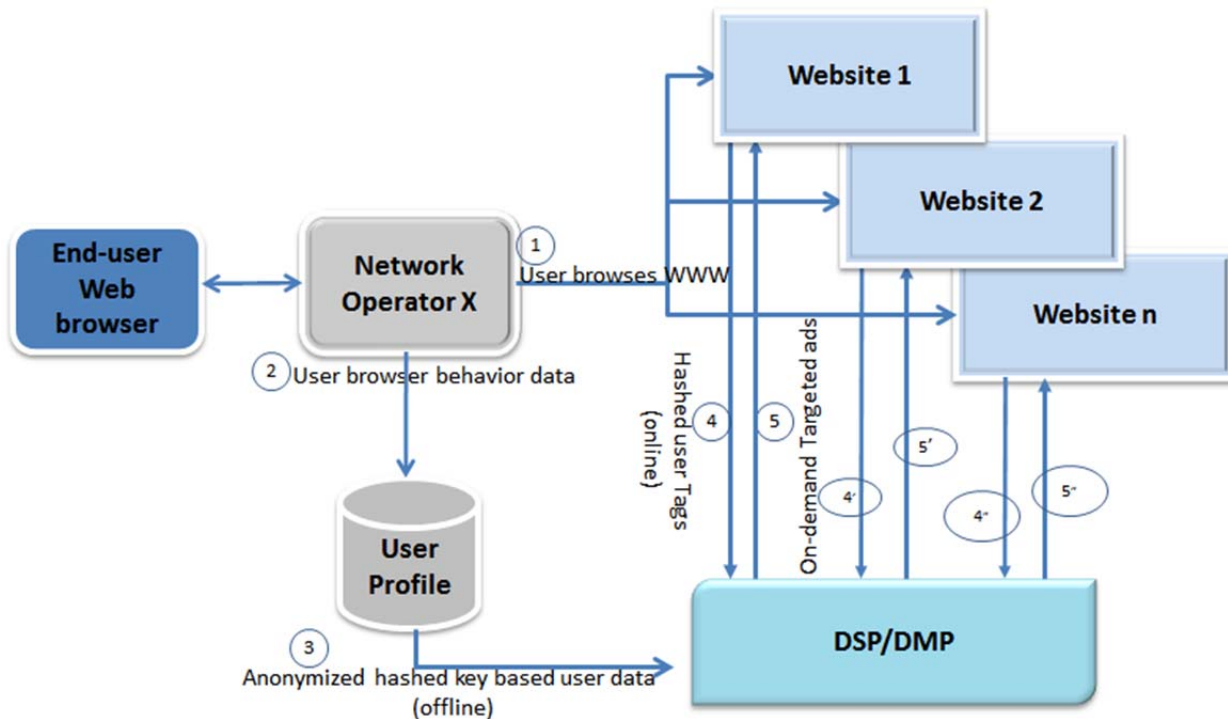


Figure 25: Relevance of Real Time Ads Example

1. User Browses the World Wide Web.
2. Network operator performs analysis of user behavior and applies algorithms if required and create a user profile for opt-in users only.
3. Send the User profile to Demand Side Platform (DSP) and/or Data Management Platform (DMP) with hashed key to protect privacy.
4. When a user browses, a hashed user tag is sent from the browser to DSP or DMP (who broker the ads)
5. DSP/DMP displays advertisement in the user browser.

9 Collaborations

9.1 Collaboration Participant Conversations

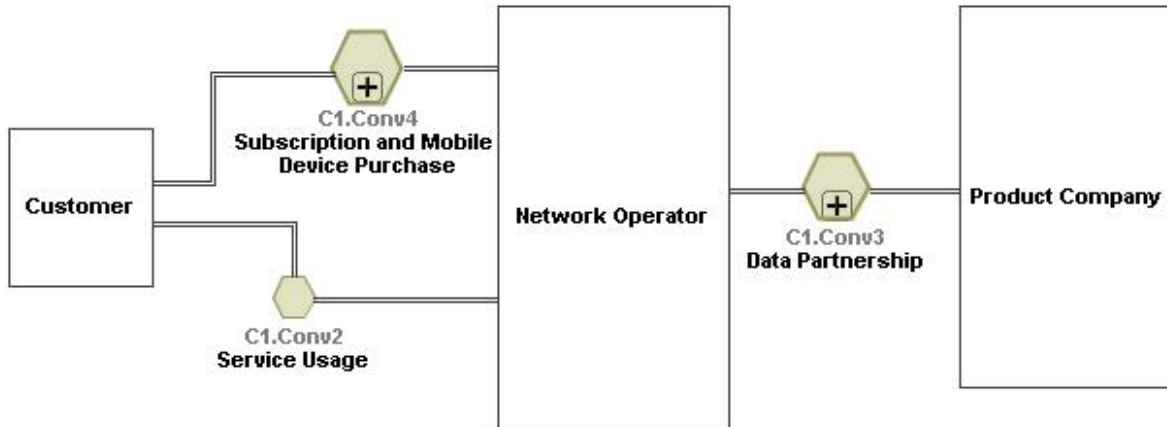


Figure 26: Data Partner Collaboration

9.1.1 Participant Conversations

This collaboration diagram shows the high level interaction among a customer, a network operator, and a product company (e.g., Mobile Game App Product Company). The main conversations are:

- Subscription and Mobile Device Purchase - Initial Customer access to the Network Operator's services;
- Service Usage - mobile device usage interactions; and
- Data Partnership - data sharing and action oriented requests (e.g., SMS advertisement).

9.2 Collaboration Subscriber NetOp Collaboration

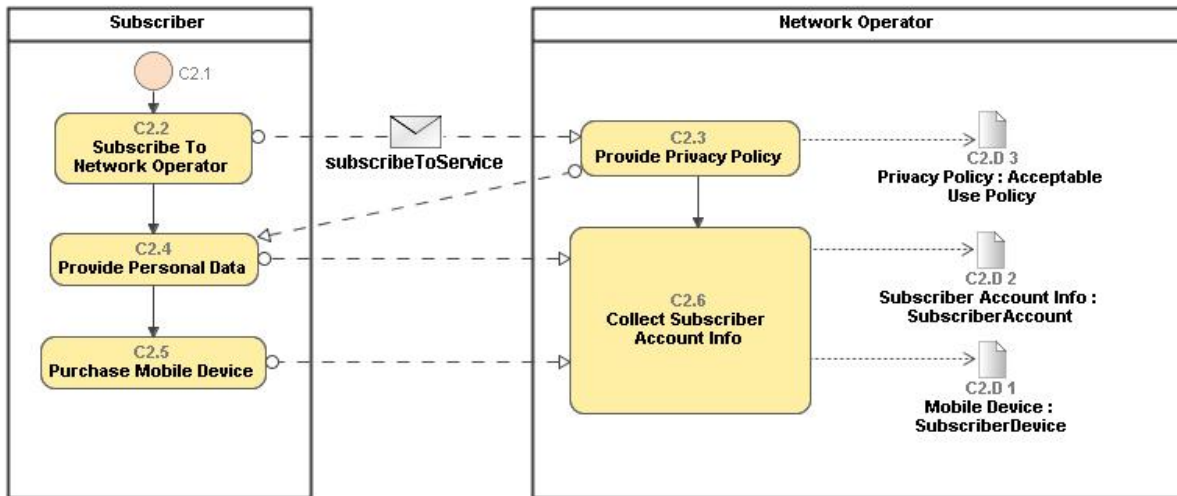


Figure 27: Diagram Subscriber NetOp Collaboration

9.2.1 Subscriber NetOp Collaboration

The Subscriber/Network Operator collaboration shows the interaction between a subscriber and a network operator at the time when a subscriber purchases wireless service and a mobile device.

9.3 Collaboration Data Partner Collaboration

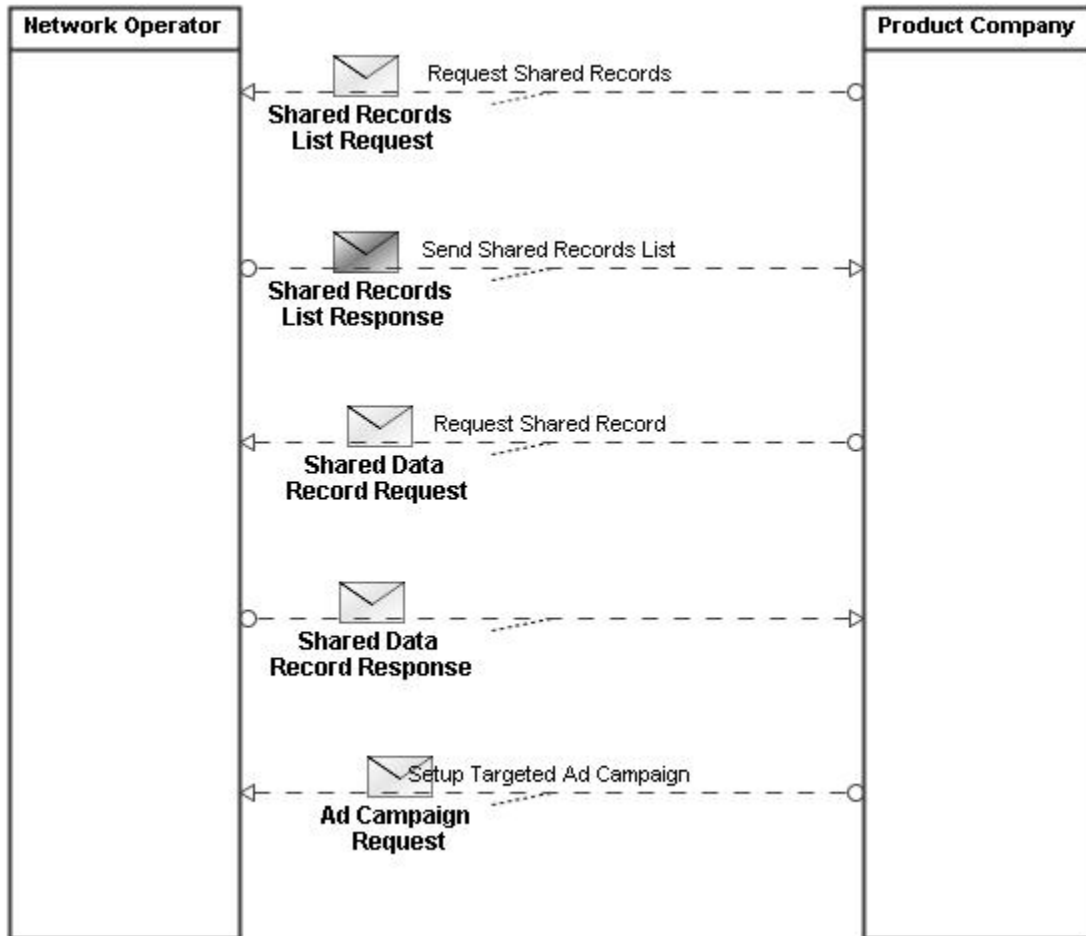


Figure 28: Data Partner Collaboration

9.3.1 Data Partner Collaboration

This collaboration depicts the data sharing and advertising campaign messages between the network operator and a product company that requests per subscriber advertising based on an aggregate subscriber target.

A Product Company requests a list of shared records from the Network Operator:

- The Network Operator responds with a list of shared records;
- The Product Company requests the data for a shared record;
- The Network Operator responds with the actual shared data and the associate metadata as well (e.g., the Acceptable Use Policy, Shared Output Record & Attributes, Context, and data provenance; and
- The Product Company follows up with a request to setup a targeted advertising campaign request to target an advertisement based on some actionable results derived from the data set that the Product Company acquired from the Network Operator.

9.4 Collaboration Per Subscriber Action Request Collaboration

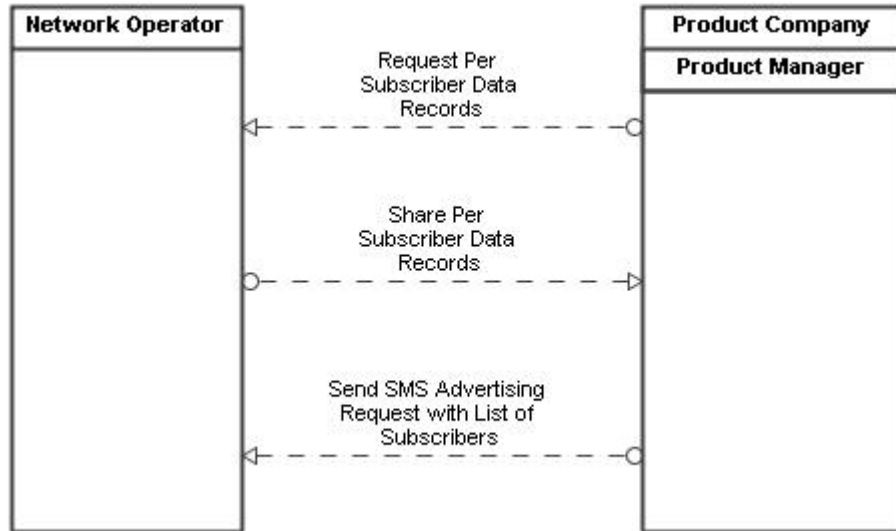


Figure 29: Per Subscriber Action Request Collaboration

9.4.1 Per Subscriber Action Request Collaboration

This collaboration depicts the high-level interaction between a typical Product Company (e.g., Mobile Game App Product Company) and Network Operator for per subscriber PII data sharing and action requests.

- Product Company request per Subscriber data records.
- Network Operator shared data at a per Subscriber level.
- The Product Company sends a request for SMS advertising with a list of subscribers. The request is made based on a derived subscriber ID rather than a phone number to protect the SMS opt-in preferences of the subscriber. That is, the Network Operator chose not to share the subscriber's mobile number with the Product Company.

10 Processes

The Retainer-Requestor Process Model Definition defines the dependencies among the various processes that take place within the owner, the requestor, or both. Data owners and data requestors are both responsible for populating their data sharing metadata. Typically, all data partners in the data value chain will at some point in time become data owners. The collection, processing, storage, and data sharing processes (responses to data sharing requests) are carried out by the data owner. This model defines shared data requests, action requests, and taking ownership of data as the main process areas implemented by all requestors. Once the requestor assumes ownership of the data, they become an owner and must employ all of the functions of the initial data owner. A requestor must then assume ownership and responsibility for the data provenance (e.g., the lineage back to the original source of the data), as well as the associated metadata that must conform to the privacy laws, regulations, and opt-in preferences of the network operator's individual customers.

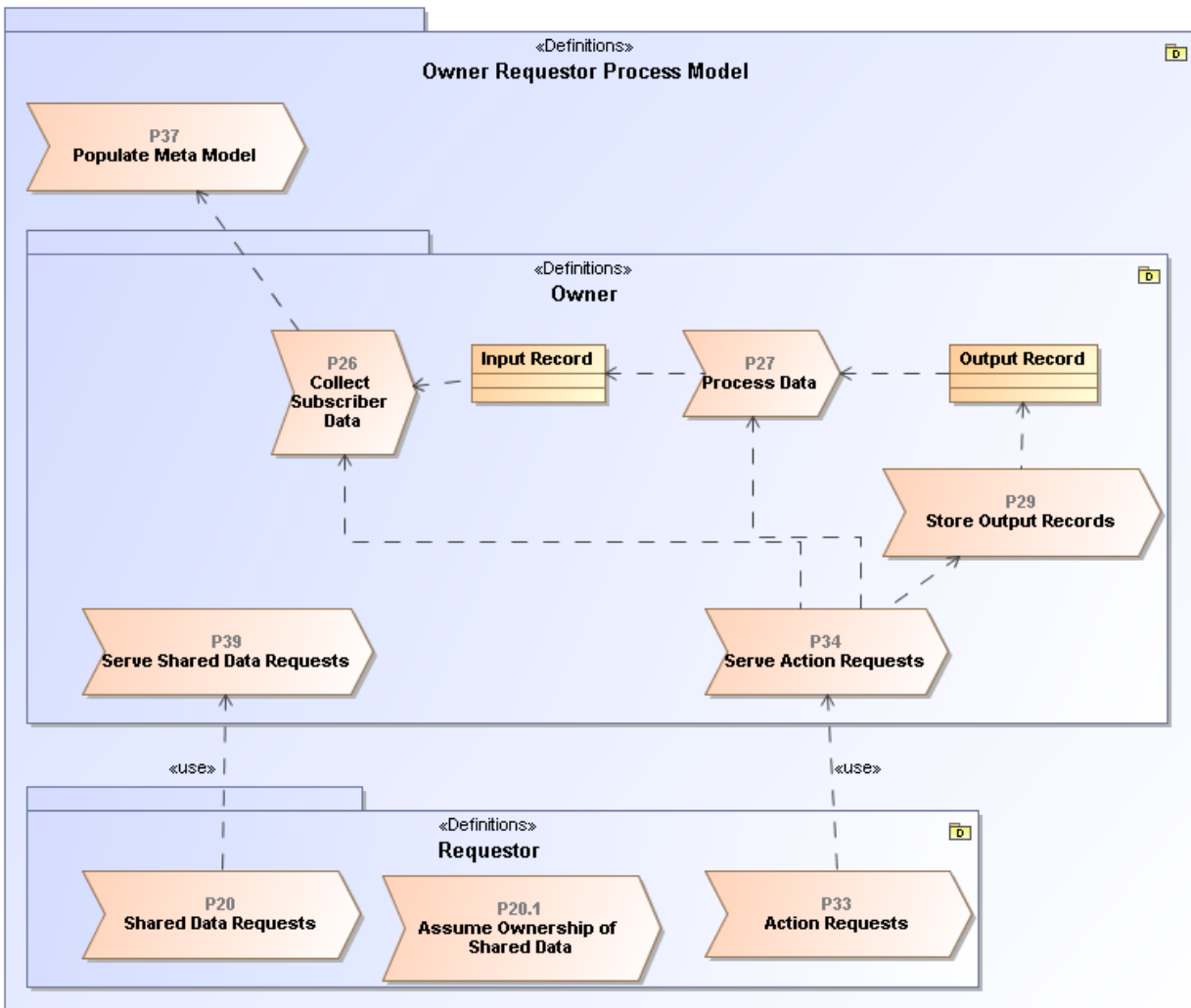


Figure 30: Retainer-Requestor Process Dependencies

10.1 Process Populate Meta-Model

The process of populating the meta-model with the appropriate metadata and policy configuration to describe the data records to be shared, sharing policies, and the context under which they can be shared.

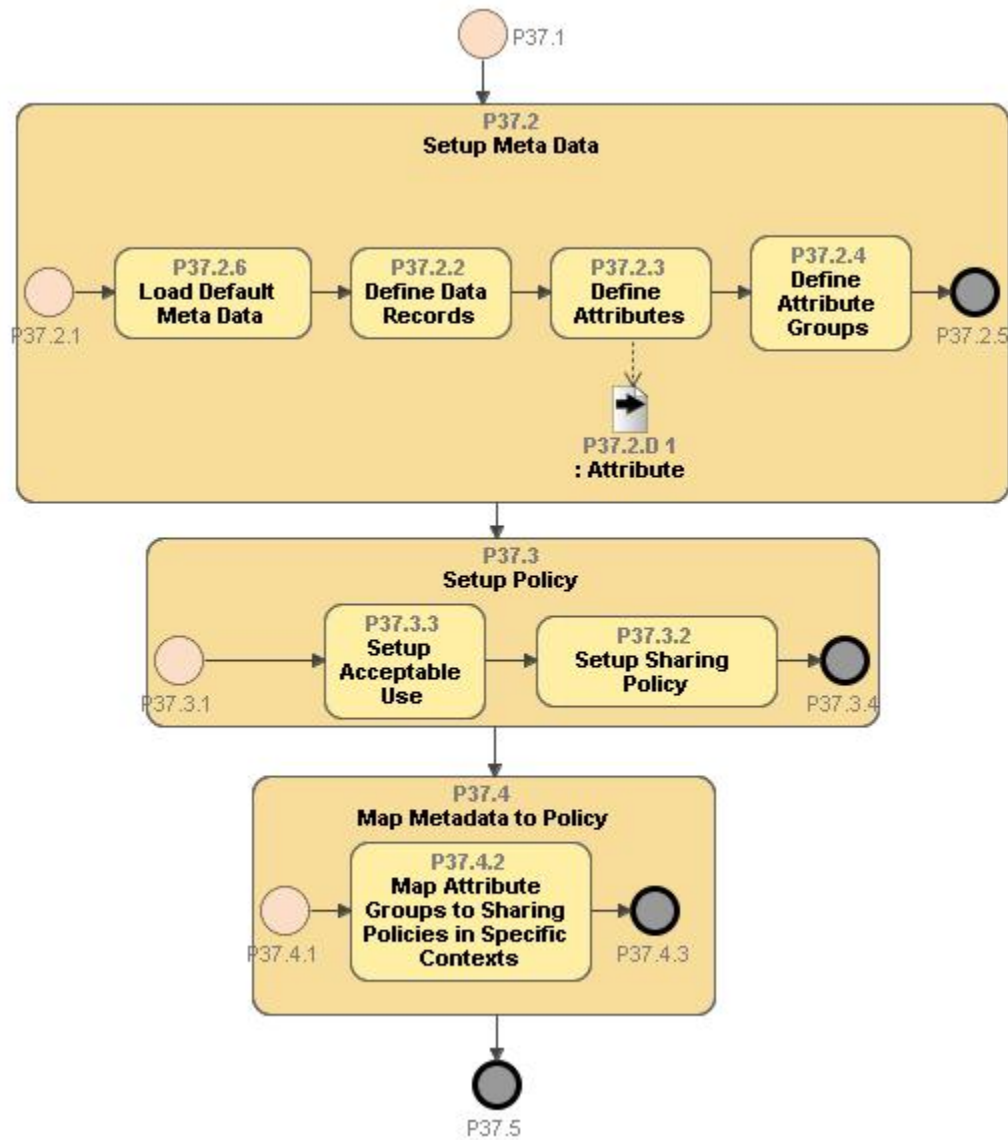




Figure 31: Populate Meta-Model Activity Diagram


All data owners must setup some minimal metadata to describe the properties of any data associated with the data owner's acceptable use and privacy policies.


- Metadata describes the data records, attributes, and attribute groups.
- Policy defines the Acceptable Use Policy and any privacy constraints on the owned data within a Context for data sharing.
- Attribute Groups are mapped to acceptable use policies and opt-in preferences for the purposes of conforming to jurisdictional laws and regulations. Moreover, this process records the provenance of data and any privacy constraints per the subscriber's preferences.


10.1.1 Process Elements


Define Attribute Groups	
Element Type	Task
Element Id	P37.2.4
Description	A business entity (owner or requestor) defines attribute groups to associate with collections of attributes that can be associated with policy.
Resources	 Post Privacy Analyst



Define Attributes	
Element Type	Task
Element Id	P37.2.3
Resources	 Post Privacy Analyst


Define Data Records	
Element Type	Task
Element Id	P37.2.2
Description	A process by which a business entity (e.g., owner or requestor) specifies the data records used in data exchanges with their related partners.
Resources	 Post Privacy Analyst


Load Default Metadata	
Element Type	Task
Element Id	P37.2.6
Description	Loads the default metadata for a particular business entity as shared or published through ATIS.
Resources	 Post Privacy Analyst




Map Attribute Groups to Sharing Policies in Specific Contexts	
Element Type	Task
Element Id	P37.4.2
Resources	 Post Privacy Analyst

Map Metadata to Policy	
Element Type	Sub Process
Element Id	P37.4
Resources	 Post Privacy Analyst

Setup Acceptable Use	
Element Type	Task
Element Id	P37.3.3
Description	Acceptable use policies must be defined per the network operator's legal agreements with subscribers, partnership agreements with data requestors, and government compliance requirements.
Resources	 Post Privacy Analyst  Post Chief Privacy Officer

Setup Metadata	
Element Type	Sub Process
Element Id	P37.2
Resources	 Post Privacy Analyst

Setup Policy	
Element Type	Sub Process
Element Id	P37.3
Resources	 Post Privacy Analyst

Setup Sharing Policy	
Element Type	Task
Element Id	P37.3.2
Resources	 Post Privacy Analyst  Post Chief Privacy Officer  Post Privacy Lawyer

Start Event	
Element Type	None Start Event
Element Id	P37.4.1

Start Event	
Element Type	None Start Event
Element Id	P37.2.1

Start Event	
Element Type	None Start Event
Element Id	P37.1

Start Event	
Element Type	None Start Event
Element Id	P37.3.1

End Event	
Element Type	None End Event
Element Id	P37.2.5

End Event	
Element Type	None End Event
Element Id	P37.3.4

End Event	
Element Type	None End Event
Element Id	P37.5

End Event	
Element Type	None End Event
Element Id	P37.4.3

Element Type	Data Output
Element Id	P37.2.D 1
Is Collection	EnumerationLiteral?

10.2 Process P37 Populate Meta-Model

The process of populating the meta-model with the appropriate metadata and policy configuration to describe the data records to be shared, sharing policies, and the context under which they can be shared.

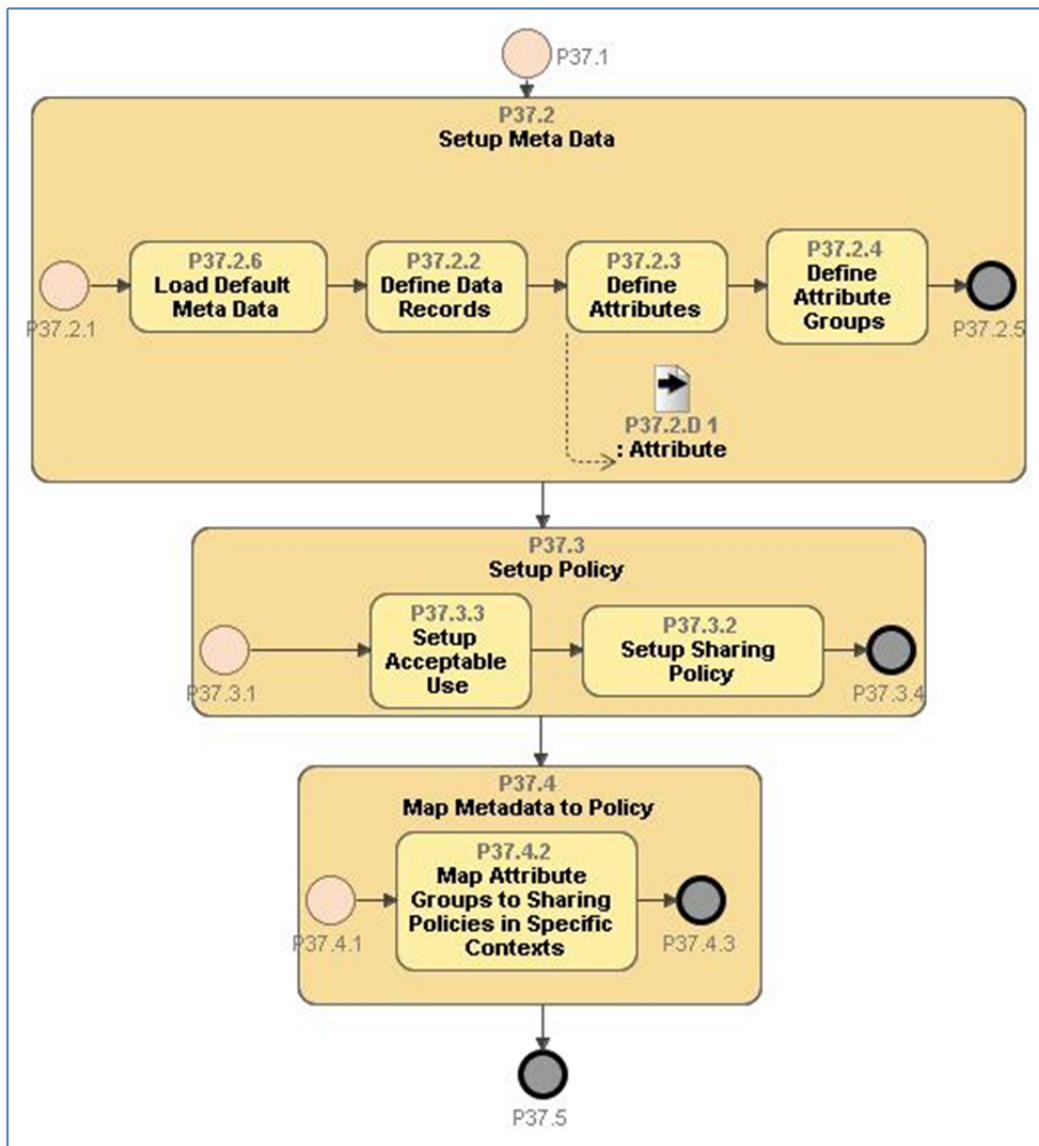












Figure 32: Process to Populate Meta-Model




10.2.1 Process Activities:

Id	Name	Description	Properties
P37.2	 Setup Metadata	NA	Resources: <ul style="list-style-type: none"> RR5 Privacy Analyst.
P37.2.2	 Define Data Records	A process by which a business entity (e.g., owner or requestor) specifies the data records used in data exchanges with their related partners.	Resources: <ul style="list-style-type: none"> RR5 Privacy Analyst.

ATIS-I-0000043

P37.2.3	 Define Attributes	NA	Resources: <ul style="list-style-type: none"> RR5 Privacy Analyst.
P37.2.4	 Define Attribute Groups	A business entity (owner or requestor) defines attribute groups to associate with collections of attributes that can be associated with policy.	Resources: <ul style="list-style-type: none"> RR5 Privacy Analyst.
P37.2.6	 Load Default Metadata	Loads the default metadata for a particular business entity as shared or published through ATIS.	Resources: <ul style="list-style-type: none"> RR5 Privacy Analyst.
P37.3	 Setup Policy	The steps to populate the sharing policy and the acceptable use policies for a network operator.	Resources: <ul style="list-style-type: none"> RR5 Privacy Analyst.
P37.3.2	 Setup Sharing Policy	NA	Resources: <ul style="list-style-type: none"> RR5 Privacy Analyst. RR4 Corporate Lawyer. RR3 Chief Privacy Officer.
P37.3.3	 Setup Acceptable Use	Acceptable use policies must be defined per the network operator's legal agreements with subscribers, partnership agreements with data requestors, and government compliance requirements.	Resources: <ul style="list-style-type: none"> RR5 Privacy Analyst.
P37.4	 Map Metadata to Policy	NA	Resources: <ul style="list-style-type: none"> RR5 Privacy Analyst.
P37.4.2	 Map Attribute Groups to Sharing Policies in Specific Contexts	NA	Resources: <ul style="list-style-type: none"> RR5 Privacy Analyst.

Data used in Process:

Id	Name	Description
P37.2.D 1	 NA[ Attribute]	 Attribute - The metadata definition of an attribute.

10.3 Service Subscription & Usage Process Definition

10.3.1 Process Wireless Service Subscription

ID:	P41
Description:	The steps collectively taken by the subscriber to subscribe to a wireless carrier and the corresponding provisioning and device activation data elements recorded and associated with the subscriber during their initial account setup.
Diagrams:	Wireless Service Subscription

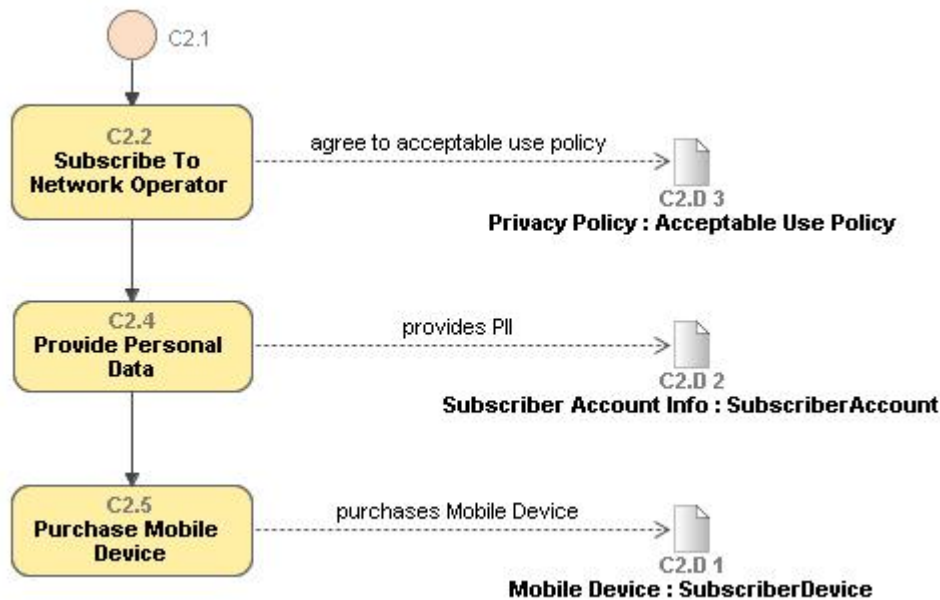


Figure 33: Wireless Service Subscription

When a customer subscribes to a network operator's wireless service, they typically share some personally identifiable information (PII) with the network operator. They are required to agree with a general acceptable use and privacy policy that defines the default acceptable use for any data collected, stored, derived, and/or shared internally and externally. The subscriber shares billing address and potentially credit card information when setting up the account. Finally, the subscriber purchases a mobile device which is immediately provisioned on the spot and associated with the subscriber. Once the subscriber starts using the device, the network operator has the capability of collecting and storing data associated with that individual subscriber via a unique device ID (e.g., IMSI, MAC Address, ESN, etc.)

10.3.2 Process Collect Subscriber Data

ID:	P26
Description:	The process by which an owner collects data about a subscriber.
Process Type:	none
Is Closed	false
Diagrams:	Collect Subscriber Data

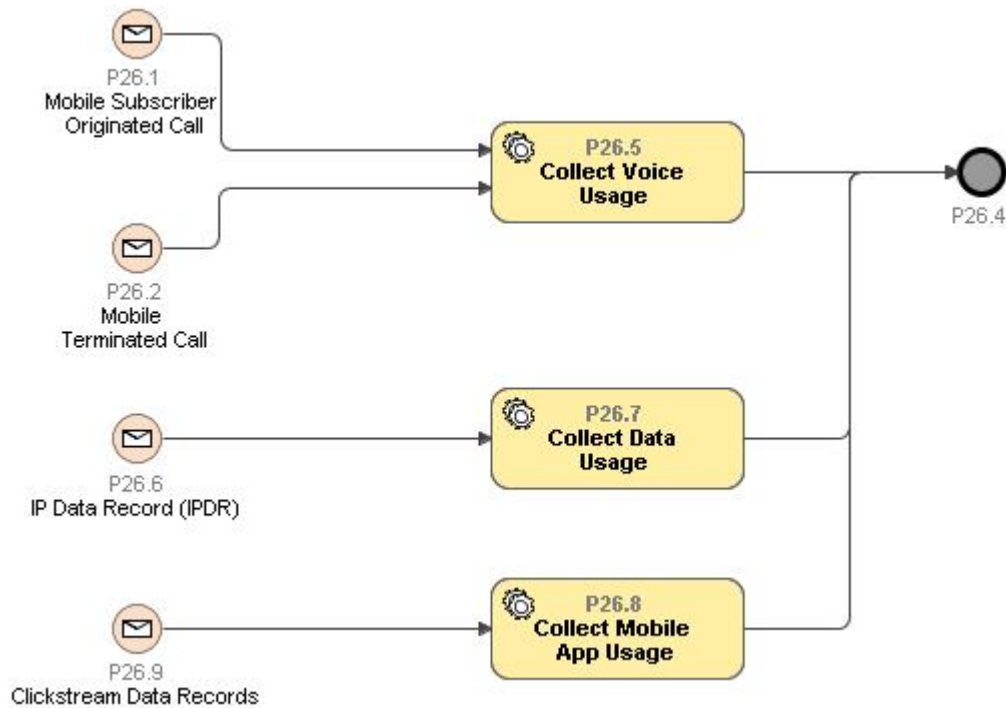


Figure 34: Collect Subscriber Data Activities

This depicts the typical Network Operator events required to collect usage data on a per-subscriber basis.

10.3.2.1 Elements descriptions:

Collect Data Usage	
Element Type	Service Task
Element Id	P26.7
Description	The Network Operator collects per-subscriber mobile data usage via IPDRs .
Implementation	Web Service

Collect Mobile App Usage	
Element Type	Service Task
Element Id	P26.8
Description	Collect per-subscriber mobile app usage by intercepting clickstream data records generated by mobile app users within the Network Operator's IP network.
Implementation	Web Service

Collect Voice Usage	
Element Type	Service Task
Element Id	P26.5
Description	Collect per-subscriber mobile voice usage (CDRs) for calls originating from or terminating to the Network Operator's Users (e.g., subscribers/customers).
Implementation	Web Service

Start Event Clickstream Data Records	
Element Type	Message Start Event
Element Id	P26.9

Start Event IP Data Record (IPDR)	
Element Type	Message Start Event
Element Id	P26.6

Start Event Mobile Subscriber Originated Call	
Element Type	Message Start Event
Element Id	P26.1
Description	Mobile network originated call placed by a subscriber.

Start Event Mobile Terminated Call	
Element Type	Message Start Event
Element Id	P26.2
Description	Mobile network intercepts a call destined to the network operator's mobile subscriber.

End Event	
Element Type	None End Event
Element Id	P26.4

10.3.3 Process Voice Usage

ID:	P42
Description:	The sequence of subscriber and network operator events as they pertain to voice usage generated by the subscriber on the operator's network.
Process Type:	none
Is Closed	false
Diagrams:	Voice Usage

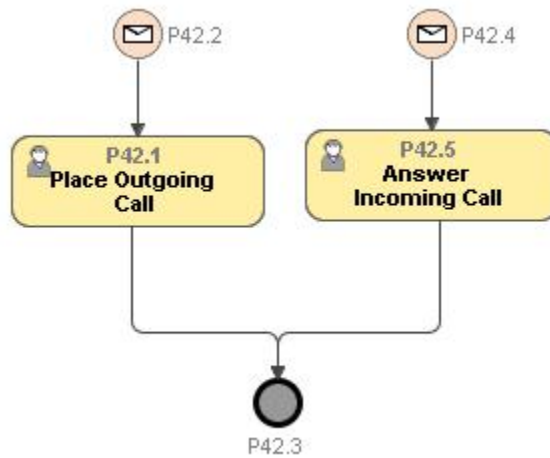


Figure 35: Voice Usage

This diagram captures the user-initiated (e.g., subscriber/customer) outgoing or incoming voice calls.

10.3.3.1 Process Elements

Answer Incoming Call	
Element Type	User Task
Element Id	P42.5
Description	The subscriber answers an incoming call on their mobile phone.
Resources	Person Subscriber Post User
Implementation	

Place Outgoing Call	
Element Type	User Task
Element Id	P42.1
Description	The subscriber places an outgoing call on their mobile phone to another party.
Resources	Post User Person Subscriber
Implementation	

Start Event	
Element Type	Message Start Event
Element Id	P42.2

Start Event	
Element Type	Message Start Event
Element Id	P42.4

End Event	
Element Type	None End Event
Element Id	P42.3

10.3.4 Process Mobile Data Usage

ID:	P43
Description:	The sequence of subscriber and network operator events as they pertain to data usage generated by the subscriber on the operator's network.
Process Type:	none
Is Closed	false
Diagrams:	Mobile Data Usage

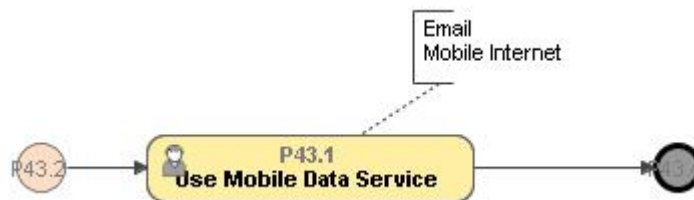




Figure 36: Mobile Data Usage

This diagram represents user-initiated (e.g., subscriber/customer) events that generate mobile data usage collected by the Network Operator.

10.3.4.1 Process Elements

Use Mobile Data Service	
Element Type	User Task
Element Id	P43.1
Description	A User (subscriber/customer) browses the Internet on their smartphone.
Resources	 Person Subscriber  Post User
Implementation	

Start Event	
Element Type	None Start Event
Element Id	P43.2

End Event	
Element Type	None End Event
Element Id	P43.4

10.3.5 Process Mobile App Usage

ID:	P46
Description:	The process by which a network operator collects mobile application usage.
Process Type:	none
Is Closed	false
Diagrams:	Mobile App Usage



Figure 37: Mobile App Usage

This diagram represents user-initiated (e.g., subscriber/customer) events that generate mobile app usage collected by the Network Operator.

10.3.5.1 Process Elements:

Use Mobile App	
Element Type	User Task
Element Id	P46.1
Description	The mobile device User (subscriber/customer) uses a mobile app which generates mobile app usage.
Resources	Person Subscriber Post User
Implementation	

Start Event	
Element Type	None Start Event
Element Id	P46.2

End Event	
Element Type	None End Event
Element Id	P46.3

Process Receive SMS

ID:	P48
Description:	The process by which a network operator intercepts and validates incoming SMS events to a subscriber.
Process Type:	none

Is Closed	false
Diagrams:	

10.4 Process Data

ID:	P27
Description:	Data processing is performed by the owner by taking a set of input attributes, processing the data, and caching or storing a set of output attributes. The data process must be configured as a set of processing steps represented as metadata.
Process Type:	none
Is Closed	false
Diagrams:	

10.5 Process Shared Data Requests

A shared data request is initiated by the requestor to a data owner.

10.6 Process Acquire Related Partner Shared Data

ID:	P35
Process Type:	
Is Closed	
Diagrams:	

10.7 Process Send SMS

ID:	P47
Description:	The process by which a network operator validates and sends SMS messages to a subscriber.
Process Type:	none
Is Closed	false
Diagrams:	

Process Action Requests

ID:	P33
Description:	The sequence of activities that make up an action request.
Process Type:	none
Is Closed	false
Diagrams:	Action Requests

10.8 Process Assume The Retainer Role for Shared Data

ID:	P20.1
Description:	The steps taken to assume the Retainer role of the data during or after data receipt from the previous Related Partner. The Retainer role may be rejected if the requestor finds that the data received does not conform to the associated metadata such as data provenance and/or acceptable use policies. If the Retainer role is rejected, the Requestor in this instance is required to delete/destroy the data.
Process Type:	none
Is Closed	false
Diagrams:	

10.9 Process Store Output Records

ID:	P29
Process Type:	none
Is Closed	false
Diagrams:	

10.10 Process Serve Shared Data Requests

ID:	P39
Process Type:	none
Is Closed	false
Diagrams:	

10.11 Process Serve Action Requests

ID:	P34
Description:	The process by which an owner of the data supports action requests associated with a particular set of data. An action request can be any action taken to engage a customer (e.g., SMS text advertisement).
Process Type:	none
Is Closed	false
Diagrams:	Serve Action Requests

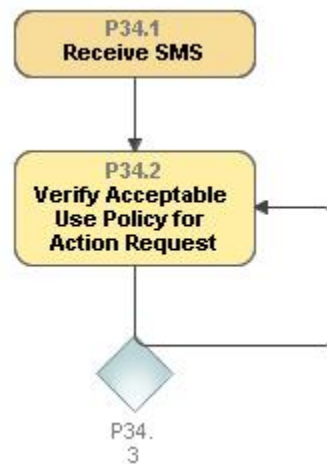



Figure 38: Serve Action Requirements

10.11.1 Elements descriptions:

Receive SMS	
Element Type	Sub Process
Element Id	P34.1
State	none
Resources	👤 Person Subscriber 👤 Post User

Verify Acceptable Use Policy for Action Request	
Element Type	Task
Element Id	P34.2
Resources	 Post Privacy Analyst

11 Acknowledgements

Jonjie Sena, TEOCO Corporation, Chair

Paul Grepps, TEOCO Corporation, BDA Reference Model Lead

We would like to acknowledge the contributions to the document from the following people:

Dan Druta – Data provenance contributions

Jim Doyle, Commscope – Use Cases

Joe Lenart, Hitachi – Privacy techniques and thorough review

Sanjay Mishra, Verizon – Relevant Advertisements Use Case

Carroll Gray-Preston – Privacy and Context contributions to the BDA reference model

12 Sources

Dwork, C. (2008). Differential Privacy: A Survey of Results. In TAMC (pp. 1-19).

Gorman, S. (2013, July 24). Move to Curb NSA Surveillance Program Defeated in House. Retrieved July 30, 2013, from WSJ Online:<
<http://online.wsj.com/article/SB10001424127887324564704578626410846098192.html>>.

Merriam-Webster Learner's Dictionary. (n.d.). Retrieved 8 28, 2013, from
<http://www.learnersdictionary.com/search/provenance>>.

Ohm, P. (2010). Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. 57 UCLA Law Review 1701.

Troianovski, A. (2013, May 21). Phone Firms Sell Data on Customers. Retrieved July 30, 2013, from online.wsj.com: <<http://online.wsj.com/article/SB10001424127887323463704578497153556847658.html>>.