D1.5 – Data Protection and Privacy Audit Report

Angel Martin

Document Number	D1.5
Status	Final
Work Package	WP 1
Deliverable Type	Report
Date of Delivery	31/12/2017
Responsible Unit	VIC
Contributors	Juan Arraiza, Angel Martin (VIC), Martin Tolan (WIT)
Reviewers	Martin Tolan (WIT), Ranjan Shrestha (TUB)
Keywords	Data Protection, Privacy
Dissemination level	PU

Change History

Version	Date	Status	Author (Unit)	Description
0.1	09/11/2017	Working	Angel Martin	ToC + initial text and "to do" calls for future contributions
0.2	23/11/2017	Working	Juan Arraiza	Section 2.1 - Updated with table of all datasets (those including personal data and all others)
0.3	14/12/2017	Working	Juan Arraiza	Updates on Executive Summary, Section 2.2 (WeFi pseudonymization), Section 2.3 (notifications to DPA), and Section 2.4 (usage rights).
0.4	24/12/2017	Working	Ranjan Shrestha	Review
0.5	26/12/2017	Working	Angel Margin	Included external expert's privacy assessment in Section 3.2 and ANNEX III.
0.6	26/12/2017	Working	Martin Tolan	TSSG/WIT inputs
0.7	28/12/2017	Working	Angel Martin	Consolidation after review
0.8	28/12/2017	Working	Martin Tolan	Review
1.0	30/12/2017	Final	Martin Tolan	Final version for release

Executive Summary

The CogNet project has a low privacy risk as it includes only datasets with no personal data except for one (WeFi) which has been pseudonymized. This deliverable explains how the appropriate data protection agency notifications have been implemented as well as which privacy and data protection measures have been put in place during research as well as during testing stages. In addition, some considerations for once the project finishes are also presented.

An assessment done by an external privacy expert on the privacy preserving methodologies and policies established in the CogNet project is also presented as part of this document. This assessment concludes that the methodologies and practices applied were appropriate to the privacy risk level of the project.

Table of Contents

1. Introduction

The guiding principles at the heart of the CogNet approach are the respect for the protection of privacy and the validity of data and its accurate representation. This research project has been conducted especially in accordance with:

- The principle of respect for human dignity and the principles of non-exploitation, non-discrimination and non-instrumentalisation,
- The principle of individual autonomy (entailing the giving of free and informed consent, and respect for privacy and confidentiality of personal data),
- The principle of justice, namely with regard to the improvement and protection of personal data,
- The principle of proportionality (including that research methods are necessary to the aims pursued and that no alternative more acceptable methods are available).
- The benefits of the studies have been conducted in proportion to the risks, and the rights and welfare of the subjects have been respected.
- The European Parliament and Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

This report describes how privacy, human and personal data protection have been managed in the CogNet project. The following sections of the document are:

- Section 2 – Data Protection: This section describes how privacy and data protection aspects of the CogNet project have been managed during the project execution.
- Section 3 – Privacy Audit: This section includes the outcome of the privacy audit conducted by an external expert at the end of the project.
- Section 4 – Conclusions: This section highlights the most important results and outcomes related to data protection and privacy management during the project.

2. Data Protection

In section 1 Introduction, the principles that have been considered when managing privacy and data protection in the CogNet project have been described. The following sub-sections present the details of how those principles have been implemented.

2.1. Datasets containing personal data

The only dataset containing pseudonymized personal data is WeFi. Its detail description can be found in ANNEX II.

2.2. Data anonymisation, pseudonymization, disassociation tools

Data anonymization has been defined as "technology that converts clear text data into a nonhuman readable and irreversible form, including preimage resistant hashes (e.g., one-way hashes) and encryption techniques in which the decryption key has been discarded[1].

In the light of Directive 95/46/EC[2] and other relevant EU legal instruments, anonymisation results from processing personal data in order to irreversibly prevent identification. In doing so, several elements should be taken into account by data controllers, having regard to all the means "likely reasonably" to be used for identification (either by the controller or by any third party).

The European Commission established Article 29 Working Party (which is the short name of the Data Protection Working Party established by Article 29 of Directive 95/46/EC). The Article 29 Working Party provides the European Commission with independent advice on data protection matters and helps in the development of harmonised policies for data protection in the EU Member States. The Working Party is composed of: (i) representatives of the national supervisory authorities in the Member States; (ii) a representative of the European Data Protection Supervisor (EDPS); (iii) a representative of the European Commission (the latter also provides the secretariat for the Working Party).

On the Article 29 Working Party opinion 05/2014 on "Anonymisation techniques"[3], the Working Party analyses the effectiveness and limits of existing anonymisation techniques against the EU legal background of data protection and provides recommendations to handle these techniques by taking account of the residual risk of identification inherent in each of them. The opinion presents the main strengths and weaknesses of the main anonymisation techniques, with the aim

---

[1] https://en.wikipedia.org/wiki/Data_anonymization

[2] http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf

[3] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

to help how to design an adequate anonymisation process in a given context. The Opinion establishes that the optimal solution should be decided on a case-by-case basis, possibly by using a combination of different techniques, while taking into account the practical recommendations developed in the Opinion.

WeFi dataset is pseudonymized as its schema contains a unique id that allows for the tracking of a "device" within the datasets. This unique id cannot be used to uniquely identify an individual as the id is specific to the vendor (TruConnect) and the format is not known outside of the vendor.

2.3. Notifications to the relevant Data Protection Agencies

2.3.1. Ireland

TSSG, part of Waterford Institute of Technology, is the Data Controller of the Wefi dataset. This dataset has been made available to the consortium partners for use in their research under the terms of the WeFi agreement and licensing. Upon auditing and validation of the dataset it was determined that that data did not contain and personably identifiable information from the subscribers (contained within the dataset) and therefore did not violate any of the data rights associated with the individuals.

Also as TSSG is contained within the same legal entity as WIT it is not required for TSSG to make an individual registration with the data protection commissioner for the control or processing of this data. In section ANNEX I – Notification receipt to the Irish Data Protection Agency, we present the statement from TSSG and WIT that explains that under the Irish Data Protection Commissioner rules it is exempt from having to register with the DPC.

2.3.2. Other countries

There is no need to notify in other countries as the rest of the partners are data processors.

2.4. Privacy and Data Protection during research stage

Below we present the implementation details followed in the CogNet project with regard to the following key principles:

1. *Data must be processed fairly, lawfully and only for the purpose for which it was collected and further processed;*

    Wefi dataset is the only dataset used for research and development purposes in the project. This dataset was legally acquired by TSSG to TruConnect, and the licensing terms can be found in ANNEX II.

    The terms and conditions of the TruConnect contract (see ANNEX II) establishes the following usage rights which allow all CogNet partners to process the data for research purposes.

SERVICES

TruConnect Technologies will provide Customer and its Authorized Users with access to the following TruConnect Technologies Data, Applications and/or Services, each as described in this Order:

PRODUCT	The Data includes information from the following datasets: 1. "WeFi Geo-Binned Data - Application and Network Usage" 2. "WeFi Network Sessions and QoS Information". The supplied data will cover New York City Metro Area. The data will be broken down into up to 6 monthly batches, each batch representing one calendar month of the year 2016 starting with July 2016 and ending with December 2016, per Customer request.
USAGE RIGHTS	Customer can use the Data for Research. Customer has the right to publish results of the research, mentioning TruConnect Technologies as source. Data usage is not limited by time. Authorized Users limited to those listed on the 5GPPP site: https://5g-ppp.eu/cognet/#

Table 1 TruConnect usage right for CogNet partners

2. *Data cannot be disclosed without authorisation unless there is an overriding act of law or legitimate grounds to do so;*

   Personal data has not been disclosed.

3. *Subject to certain exemptions, individuals have a right to access the information relating to them and to ask for correction of inaccurate data;*

   Data anonymisation, pseudonymization, and disassociation tools, as presented in section 2.2, were used to remove personal data from the WeFi dataset.

4. *Information cannot be transferred beyond the EEA boundaries without consent or adoption of other adequate protection measures;*

   The Article 29 Working Group views the State of Israel as a country that guarantees the same standard of Data Protection and treatment of Personal Data as within the European Union. The Article 29 Working Group has published a number of communiques clarifying that the transfer of data to and from Israel poses no obstacle under current EU Data Protection Legislation.

5. *Organisations are usually required to register or notify the processing of personal data unless the data processing is simplistic, or a data protection officer has been appointed;*

   See section 2.3.

6. *Organisation must have adequate security measures in place.*

   Firstly, data that identifies individuals (personal data) will not be kept any longer than strictly necessary. TSSG, as Data Controller of the WeFi dataset, to protect personal data against accidental or unlawful destruction, loss, alteration and disclosure, particularly when processing involves data transmission over networks, has implemented the following security measures to ensure a level of protection appropriate to the data:

   - Data has been stored in a server, hosted at TSSG datacentre, which includes physical access control measures.

- Access to data was given only to those individuals that met the "need-to-handle" principle.
- Transmission over networks was done using encrypted protocols such as HTTPS, VPN, or FTPS.

2.5. Privacy and Data Protection during testing stage

The datasets employed along the testing stage within CogNet is compiled in the table below. Here, it can be seen that all of them are Experimental data (non-synthetic from labs and equipment) or Derived data (non-synthetic after data mining or statistical analysis.) So, none of them contains personal data and in the Derived case from WeFi dataset the derived data already ships a disassociation mechanism to turn any real-world identifier into a synthetic machine learning record. This means that no personal data is processed or stored and without the need of applying specific privacy and data protection mechanism beyond the corporative login and credentials control applied by each entity in the research facilities.

Demo	Generation Type	Contains Personal Data	Anonymised	Data Sample Features (generated by the controller)	Metadata (produced by the processor)
Follow The Sun	Experimental	No	Not applicable	CPU, I/O, VMs	Noisy VM (Create Alarm on Vitrage)
Massive Multimedia Content Consumption - Media SLA	Experimental	No	Not applicable	VM Network, CPU, Memory and Disk	Migrate VNF or scale up (it depends on the violated SLO)
Massive Multimedia Content Consumption - Synthetic Classification	Experimental	No	Not applicable	L2-L4 traffic (5 tuples features)	Inform Flow Type
Massive Multimedia Content Consumption - Topology Optimization	Experimental	No	Not applicable	BW & Latency & Network topology Graph	Optimal Topology
Dense Urban Area	Simulation	No	Not applicable	VM CPU	Create Alarm
Detection And Reparation Of Network Threats	Experimental	No	Not applicable	Traffic flow metrics	Remove end device (SFC) Deploy local

				(sflow, netflow)	ACL (SFC)
Connected Cars	Simulation	No	Not applicable	L1-L3 Traffic data inside the cells	Redirect Antenna
Urban Mobility Awareness	Derived	No	Disassociation	Throughput of Mobile session, hourly weather and PoI	Create heatmaps Predict geo-based demands

Table 2 – Generation, processing and personal aspects of CogNet Datasets

Table 2 – Generation, processing and personal aspects of CogNet DatasetsError! Reference source not found. shows that the nature of data employed across the testing on the demonstrators is not related to personal data generating non-synthetic data from labs and equipment.

2.6. Privacy and Data Protection considerations for once the project finishes and if the technologies are implemented in an operational (real) environment

The notion and understanding of privacy will continue to evolve. Data collection and utilization have already been, and continue to be, even more pervasive, in some cases with the individual's consent, but in many cases without the individual's knowledge. Debates will continue about privacy on one hand and efficiency and convenience on the other. New or updated regulatory requirements are expected to emerge as well.

In this ever-changing scenario, organisations should establish and follow a comprehensive privacy audit methodology to ensure that they are not inadvertently exposed to any undesired risk. Furthermore, steps should be taken to ensure that all privacy-related risk is minimized to an acceptable level. Organisations should also be wary of emerging technological trends and their impact on privacy. Consideration should be given to include privacy audit in the annual audit plan, and reports should be provided on a periodic basis to all stakeholders.

3. Privacy Audit

Privacy audits aim at assessing how organizations implement privacy protection management to comply with regulatory requirements or international best practices and widely-accepted principles (Cavoukian, 2016) as well as to check compliance with the organization's own privacy-related policies.

A privacy audit includes, among other things, evaluating procedures undertaken by an organization throughout the typical information life-cycle phases: how information is handled, including acquisition, reception, distribution, use, maintenance and eventually disposal. A privacy audit presents the status of risk associated with potential information misuse and makes recommendations about initiatives that can limit that risk, including the organization's liability or reputational risk.

Privacy and confidentiality have distinct meanings. Confidentiality can be referred to as the protection of information sharing without the express consent of the owner. On the other hand, privacy refers to the freedom from intrusion into private matters.

3.1. Privacy Audit Methodology

Muzamil (2014), presents some high-level steps of a methodology that can be adopted to conduct a privacy audit, which are illustrated in Figure 1 below and which are presented in this section.

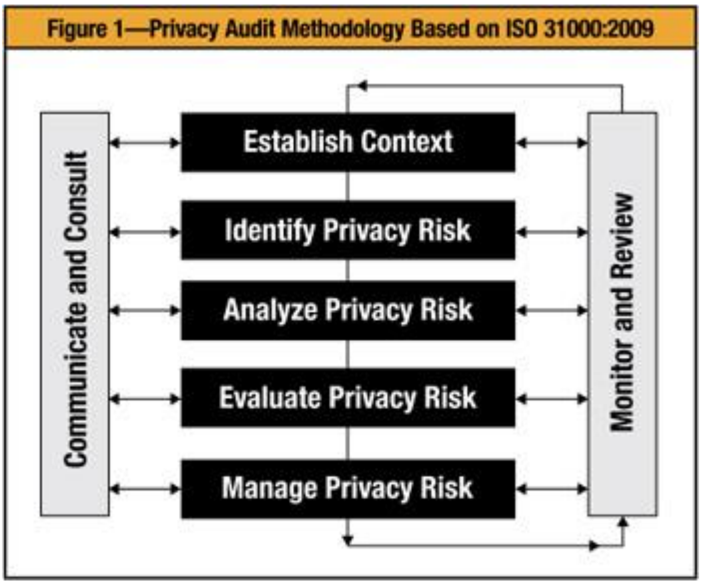

Figure 1 Privacy audit Methodology

The related considerations for each step are as follows:

3.1.1. *Establish context*

A key challenge in any privacy-related discussion is that it is a very subjective phenomenon. A substantial amount of grey area always creeps in whenever attempts are made to define privacy, as there is no universally agreed-upon understanding. The interpretation may vary significantly by country, culture or organization. For instance, most organizations nowadays set up a banner notification on computer login screens about monitoring the activities of the user and deploy some sort of technical tools on their network for this task. However, it is debatable to what extent the organization can utilize these data. Some argue that monitoring data (e.g., search terms, web sites visited, products purchased) on an organization's resources (e.g., computer, Internet) during official working hours is not a violation of privacy, even if the company sells these data to an external party. Others term such actions as intrusion of privacy. The paramount question of who is the data owner (the organisation that collected the data or the individual[s] who produced the data) is given a fair amount of consideration. It is imperative for privacy auditors to ensure that all stakeholders are aligned to the criteria used and the outcome of the proposed privacy audit.

3.1.2. *Identify privacy risk*

The next step is to identify privacy-related risk by utilizing the usual risk identification tools, techniques and methods. Although listing all possible privacy risk is beyond the scope of this report and may not be practical, the following emerging risk areas should be part of this step.

3.1.2.1 Operating model: Cloud VS in-house

Hosted computer solutions (cloud computing) are increasingly considered by corporations. Without a reasonable degree of research, judgments are swiftly promulgated about the perceived evils of the hosted solutions. Auditors should objectively review the associated risk and assign the risk rating accordingly, keeping in mind that the concept of hosted solutions is neither novel nor abstract. Furthermore, cloud computing is not inherently bad news for privacy concerns. Such concerns are based on the unfounded belief that data kept in-house are somehow more secure. As a matter of fact, the security of data is dependent upon the security measures utilized by the organization and not on location—in-house or in the cloud.

3.1.2.2 Social media

Social media has provided an excellent way for companies to communicate with their customers and stakeholders on a timely basis. However, as is possible for personal social media accounts where information from different sources can be aggregated to reveal sensitive information, it may be possible for companies to be publishing seemingly innocuous information, but when combined or correlated with other sources, the information disclosed is private.

3.1.2.3 Mobile devices

The skyrocketing ownership of smart mobile devices has given rise to security concerns related to bring your own device (BYOD). From a privacy perspective, the following points are worth extra consideration:

3.1.2.3.1 Location data

The integration of navigation systems in the inherent cell-tower triangulation position system has raised some genuine privacy concerns. Geolocation data from mobile devices are considered to be sensitive. These data can be used for (unwanted) marketing to consumers based on location or for tracking the movement of users. Different guidelines are being developed to address the privacy of location-based data.

3.1.2.3.2 Hardware identifiers

Mobile apps can access unique hardware identifiers for marketing and other communication purposes to the consumer[4]. Permission for such tracking might not have been explicitly granted by the owner of the device.

3.1.2.3.3 Personal utilities or games

Some mobile apps can gain unwarranted access to the utilities on the phone, which are not required for the intended purpose of installing the application[5].

3.1.2.4 Big data

The rapid enhancements in data collection and analytics technologies are resulting inversely in privacy erosion. Sophisticated tools can correlate data from different sources to identify personal or private information. The data warehouse created to analyse and provide business benefits can also result in unintended leakage of private information.

3.1.2.5 Conflict with other laws

Data privacy requirements can sometimes conflict with other laws, e.g., data retention laws[6].

3.1.3. Analyse privacy risk

Risk analysis predominantly consists of performing two steps:

1. Assign inherent risk rating.
2. Evaluate implemented controls.

Inherent risk rating can be assigned to each risk using an impact/consequence and probability matrix (see example in Figure 2).

---

[4] https://www.finjanmobile.com/mobile-device-ad-tracking/

[5] http://www.channelfutures.com/mobile-computing/study-mobile-app-data-mining-bigger-threat-malware

[6] http://www.lexxion.de/pdf/edpl/EDPL%20Reading%20Sample_Maja%20Brkan.pdf

Figure 2—Inherent Risk Rating Matrix						
		Consequence/Impact				
		1—Notable	2—Minor	3—Moderate	4—Major	5—Severe
Probability	5—Definitely	Moderate risk	Significant risk	Significant risk	Extreme risk	Extreme risk
	4—Likely	Moderate risk	Significant risk	Significant risk	Extreme risk	Extreme risk
	3—Possible	Moderate risk	Moderate risk	Significant risk	Significant risk	Extreme risk
	2—Unlikely	Low risk	Moderate risk	Significant risk	Significant risk	Extreme risk
	1—Rare	Low risk	Low risk	Moderate risk	Moderate risk	Significant risk

Figure 2 Inherent Risk Rating Matrix

The effectiveness and efficiency of implemented controls should be assessed to evaluate the degree of risk mitigation. Examples of privacy controls that an organization may have or may wish to implement include, but are not limited to:

3.1.3.1 Privacy policy

In the context of a collaborative research project, a privacy policy should be documented, approved and communicated to all project members and stakeholders. In addition to taking any regulatory requirements into consideration, the policy should disclose management's intention on information collection and its subsequent usage.

3.1.3.2 Database privacy controls

Cell suppression, partitioning, noise and perturbation are some of the techniques that can be used to mitigate risk associated with inference and aggregation attacks. In these kinds of attacks, information from different sources (e.g., phone records, social network sites) is linked to disclose private information. Techniques such as privacy integrated queries (PINQ) could be used to provide privacy for underlying records.

3.1.3.3 Cryptography

As required by several standards, including the Payment Card Industry Data Security Standard (PCI DSS), all personally identifiable information (PII) has to be stored in an encrypted format to prevent misuse or unauthorized access to such information.

3.1.4. Evaluate privacy risk

The residual risk is calculated based on inherent risk and control ratings. Residual risk is the level of risk that remains after taking into account all existing controls. Figure 3 shows a suggested equation for residual risk calculation.

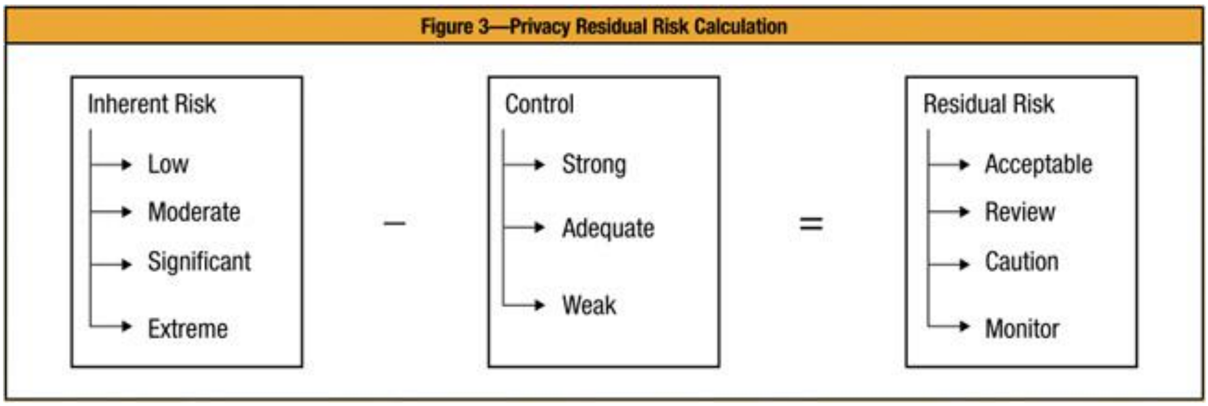

Figure 3 Privacy Residual Risk Calculation

3.1.5. Manage privacy risk

This step is primarily performed by management, and the auditor's role generally is to ascertain the adequacy of the steps taken to mitigate risk. Using residual risk rating as a basis, risk management initiatives can be identified. Such initiatives might include strengthening the current controls or implementing new controls to mitigate privacy-related risk. There are several forms of risk management, such as avoidance, transfer or reduction to an acceptable level, after taking into consideration the cost vs. benefit of the risk treatment.

3.1.6. Communicate and consult

Periodic reports should be provided to management, the audit committee and any other stakeholder during each phase of the methodology. Any major areas of concern should be brought to management's attention immediately.

3.1.7. Monitor and review

The performance of the privacy risk management system should be continuously monitored. Regulatory requirements, internal processes and business processes might change, which, in turn, could affect privacy risk management practices. Appropriate monitoring and review processes should be completed throughout the risk management process to ensure that all decisions are made based upon current and up-to-date information.

3.2. CogNet's Privacy Audit

The CogNet project includes only datasets with no personal data except for one (WeFi) which has been pseudonymized. Besides, the consequence/impact of such risk would go from "1-Notable" to "3-Moderate" (see Figure 2), as the sensitivity of the personal data contained in the original datasets was in the range of low to medium.

Because of the aforementioned low probability and low-to-medium consequence/impact, the overall rating of the privacy risk is "low". In addition, adequate risk control (privacy preserving) measures that have been implemented (as presented in section 2 - Data Protection), therefore the residual risk can be considered as “acceptable”.

In ANNEX III – Privacy Assessment Audit a privacy assessment report can be found.

4.Conclusions

The CogNet project has not handled much personal data. The datasets employed along the testing stage within CogNet are Experimental data (non-synthetic from labs and equipment) or Derived data (non-synthetic after data mining or statistical analysis). Only the WeFi dataset has pseudonymized data, and thus, the privacy risk level is (very) low, as it can be also seen in the privacy audit conducted by an external expert and presented in section 3 - Privacy Audit.

Nonetheless, in this report we have described how privacy and data protection aspects have been appropriately handled during the project execution and we have also presented considerations for managing privacy and data protection beyond the duration of the project (section 2.6 - Privacy and Data Protection considerations for once the project finishes and if the technologies are implemented in an operational (real) environment).

REFERENCES & BIBLIOGRAPHY

1. European Commision; Protection of Personal Data; http://ec.europa.eu/justice/data-protection/
2. ENISA; Privacy and Data Protection by Design; January 12, 2015; https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design
3. Ann Cavoukian; Privacy by Design - The 7 Foundational Principles: Implementation and Mapping of Fair Information Practices; July 7, 2016; https://gpsbydesign.org/resources-item/the-7-foundational-principles-implementation-and-mapping-of-fair-information-practices/
4. Muzamil Riffat; Privacy Audit—Methodology and Related Considerations – ISACA Journal Volume 1, 2014; https://www.isaca.org/Journal/archives/2014/Volume-1/Pages/Privacy-Audit-Methodology-and-Related-Considerations.aspx?utm_referrer=

ANNEX I – Notification receipt to the Irish Data Protection Agency

Within the Republic of Ireland the office of the Data Protection Commission is the government department that is responsible for upholding the rights of individuals as set out in Irish law, and enforcing the obligations upon data controllers within the state. All organisations within the state that are controllers or processers of data must register with the data protection commissioner as a data controller/processor. Within the relevant legislation exemptions exist based on the type of organisation and for the nature of the data held by organisations.

As the TSSG (Telecommunications Software & Systems Group) is held under the same legal entity as WIT (Waterford Institute of Technology) TSSG is therefore exempt from having to hold a unique registration with the data protection commissioner and furthermore is exempt from registering with the commissioner due to the nature of the organisation. There is no need for the TSSG/WIT to register with the data protection commissioner as both organisations are regarded as being third level educational institutions.

Further details are available directly from the data commissioner's web site[7] and a comprehensive list of all the exemptions are also available from the text of the legislation[8] itself known as "*S.I. No. 657/2007 - Data Protection Act 1988 (Section 16(1)) Regulations 2007*".

[7] https://www.dataprotection.ie/docs/Who-is-required-to-Register/1089.htm

[8] http://www.irishstatutebook.ie/eli/2007/si/657/made/en/print

ANNEX II – Wefi purchase contract & Wefi dataset license terms

A.1. Wefi purchase contract

TruConnect Technologies LLC

ORDER AGREEMENT

This Order Agreement between Waterford Institute of Technology ("Customer") and TruConnect Technologies LLC, as of August 2016 will be subject to the terms and conditions set forth in the End User License Agreement in Appendix C

CUSTOMER (COMPANY NAME)		PRIMARY CUSTOMER CONTACT NAME	Robert Mullins
STREET ADDRESS OR PO BOX		EMAIL	rmullins@tssg.org
FLOOR, SUITE		PHONE	
CITY		DEPT CODE OR PO#	
STATE		BILLING CONTACT	
ZIP		BILLING EMAIL	
COUNTRY		BILLING PHONE	

AGREEMENT TYPE (CHOOSE ONE)		CUSTOMER USE ONLY	X	AGENCY		RESELLER/PARTNER

SERVICES

TruConnect Technologies will provide Customer and its Authorized Users with access to the following TruConnect Technologies Data, Applications and/or Services, each as described in this Order:

PRODUCT	The Data includes information from the following datasets. 1. "WeFi Geo-Binned Data - Application and Network Usage" 2. "WeFi Network Sessions and QoS Information". The supplied data will cover New York City Metro Area. The data will be broken down into up to 6 monthly batches, each batch representing one calendar month of the year 2016 starting with July 2016 and ending with December 2016, per Customer request.
USAGE RIGHTS	Customer can use the Data for Research. Customer has the right to publish results of the research, mentioning TruConnect Technologies as source. Data usage is not limited by time. Authorized Users limited to those listed on the 5GPPP site: https://5g-ppp.eu/cognet/#
DATA DESCRIPTION	The WeFi Geo-Binned Data – Application and Network Usage dataset contains information on application and network usage on mobile devices, broken down by 10x10 meter location and hourly bins. The WeFi Network Sessions and QoS Information datasets contains information on network usage, broken down into sessions, measured from Connect to Disconnect. There are two separate datasets – one for Cellular network connections and another one for Wi-Fi network connections
DATA FIELDS	As specified in Appendix A and Appendix B
REPORTING PERIOD	Up to 6 calendar months.
FORMAT	CSV
FILE TRANSFER	FTP or Google Cloud Storage Links
DATA CONTACT/RECIPIENT	Robert Mullins, rmullins@tssg.org

CONFIDENTIAL – ORDER AGREEMENT – 1 OF 2

A.2. Wefi dataset license terms

Below we insert (copy-paste) the text of the Wefi dataset licensing terms as found at http://www.truconnect.com/legal-terms-and-conditions-personal/wefi/ on 14/12/2017.

Terms & Conditions (http://www.truconnect.com/legal-terms-and-conditions-personal/)
Hearing Aid Compatibility (http://www.truconnect.com/legal-accessibility/)
Customer Proprietary CPNI Policy (http://www.truconnect.com/legal-consumer-protection/)
Privacy Policy (http://www.truconnect.com/legal-privacy-policy/)
Global Texting Countries (http://www.truconnect.com/legal-global-texting/)
Law Enforcement (http://www.truconnect.com/legal-law-enforcement-requests/)
Open Internet Statement (http://www.truconnect.com/open-internet-statement/)
We – Terms of Service (http://www.truconnect.com/legal-terms-and-conditions-personal/we /)
California LifeLine program (http://www.truconnect.com/ca-lifeline-notice/)

We – Terms of Service

IMPORTANT - PLEASE READ THE TERMS OF SERVICE FOR THIS SOFTWARE LICENSE AGREEMENT ("AGREEMENT") CAREFULLY. IF YOU DO NOT AGREE TO ALL TERMS AND CONDITIONS OF THIS AGREEMENT YOU SHOULD DISCONTINUE THE DOWNLOAD AND/OR THE USE OF THE TRUCONNECT TECHNOLOGIES SOFTWARE BY DISABLING THE TRUCONNECT TECHNOLOGIES SOFTWARE UNDER YOUR DEVICE'S SETTING.

This Agreement is a legal agreement between you, the end user ("End User" or "you") and Truconnect Technologies, LLC, located at 1149 S. Hill St., Suit H-400, Los

Angeles, CA 90015, USA ("Truconnect Technologies", "us", "we" or "our"), for Truconnect Technologies Software includes computer software, including we or Beta Truconnect Technologies Software (as de ned below) and "online" or electronic documentation (collectively, the "Truconnect Technologies Software"). By downloading or continuing to use the preinstalled Truconnect Technologies Software you agree to be bound by the terms of this Agreement. If you do not agree to the terms and conditions of this Agreement, do not download or continue the use of the Truconnect Technologies Software.

WITH RESPECT TO BETA OR OTHER PRE-PRODUCTION VERSIONS OF THE TRUCONNECT TECHNOLOGIES SOFTWARE (THE "BETA TRUCONNECT

TECHNOLOGIES SOFTWARE"), YOU UNDERSTAND THAT THE BETA TRUCONNECT TECHNOLOGIES SOFTWARE MIGHT HAVE BUGS AND/OR LIMITED

FUNCTIONALITY AND THAT ONE OF THE PURPOSES OF THE PRE-RELEASE BETA TEST IS TO RECEIVE FEEDBACK FROM END USERS REGARDING THE BETA

TRUCONNECT TECHNOLOGIES SOFTWARE AND LIMITATIONS AND PROBLEMS THEY MAY ENCOUNTER TO HELP US TO FURTHER DEVELOP THE BETA TRUCONNECT TECHNOLOGIES SOFTWARE AND YOU ARE WILLING TO PARTICIPATE IN THE PRE-RELEASE BETA TEST OF THE TRUCONNECT TECHNOLOGIES SOFTWARE.

1. License - Subject to the terms of this Agreement and limited to the duration of the pre-release beta test, as applicable and as designated on the webpage where you downloaded the Beta Truconnect Technologies Software (the "Beta Test Period"), we grant you a non-transferable, non-exclusive, non-sublicensable, royalty-free and fully paid, worldwide right and license to install one (1) copy of the Truconnect Technologies Software on one (1) computer or mobile device, as applicable, in executable object code format only, solely for your own private use or internal business operations. The Truconnect Technologies Software is licensed, not sold, for your use. Your license confers no title or ownership in the Truconnect Technologies Software and should not be construed as any sale of any rights in the Truconnect

Technologies Software. During the Beta Test Period, we may, in our sole discretion, notify you, either by sending you an e-mail or by a notice on the Truconnect Technologies and/or its affiliates' website, that we have released an updated version of the Beta Truconnect Technologies Software. Upon your receipt of such noti cation, you agree to download the updated version of the Beta Truconnect Technologies Software and to use such version instead of the prior version. Any updated version of the Beta Truconnect Technologies Software will be considered "Beta Truconnect Technologies Software" for purposes of this Agreement.

2. Term - The term (the "Term") of this Agreement shall commence upon your acceptance of the terms of this Agreement through your installation or rst use of the Software and shall either continue until terminated, or, in the case of Beta Truconnect Technologies Software, until expiration of the Beta Test Period (unless earlier terminated in accordance with the terms and conditions of this Agreement).

3. Restrictions - The rights granted to you in this Agreement are subject to the following restrictions: (a) You shall not license, sell, rent, lease, transfer, assign, distribute, display, host, outsource, disclose or otherwise commercially exploit or make the Truconnect Technologies Software available to any third party; (b) You shall not modify, make derivative works of, disassemble, reverse compile or reverse engineer any part of the Truconnect Technologies Software; (c) You shall not access the Truconnect Technologies Software in order to build a similar or competitive product or service or to publish any performance or benchmark test or analyses relating to the Truconnect Technologies Software; (d) and except as expressly stated herein, no part of the Truconnect Technologies Software, including, but not limited to, any copyright, trademark, patent, or other intellectual property or proprietary rights, may be copied, altered, reproduced, distributed, republished, downloaded, displayed, translated, posted or transmitted in any form or by any means, including but not limited to electronic, mechanical, photocopying, recording or other means. You may not separate the component parts of the Truconnect Technologies Software for use on more than one (1) computer or mobile device, as applicable. You shall be solely responsible for the storage of any and all

data and information with respect to the Truconnect Technologies Software. It is your sole responsibility to back-up to another secure location, on a regular basis, any data les concerning your use of the Truconnect Technologies Software. Truconnect Technologies is in no way responsible for protecting and/or backing-up such information and shall have no liability for lost or corrupt data.

4. Charges and Billing - Truconnect Technologies may charge subscription or other fees to access certain Truconnect Technologies services. If you must pay a subscription or other fee to access a Truconnect Technologies service, this information will be posted on the Website established for such Truconnect Technologies

service or the distribution of such Truconnect Technologies service and/or within this Agreement. YOU ACKNOWLEDGE THAT SUCH FEES ARE PAYABLE IN

ADVANCE AND ARE NOT REFUNDABLE IN WHOLE OR IN PART. YOU AGREE THAT YOU ARE FULLY LIABLE FOR ALL CHARGES TO YOUR ACCOUNT,

INCLUDING ANY UNAUTHORIZED CHARGES. You agree to reimburse Truconnect Technologies for all costs and expenses incurred by Truconnect Technologies in connection with the collection of payments, including bank or service charges and reasonable attorney fees, if any. If your use of the Truconnect Technologies services is subject to use or sales tax, you agree that Truconnect Technologies may also charge you for any such taxes, in addition to other applicable fees. By purchasing a Truconnect Technologies service, you represent that you are at least the age of majority in your place of residence (i.e. 18 years of age in the United States).

5. Carrier Charges - You acknowledge that (i) the Truconnect Technologies Software will facilitate the exchange of information to and from your mobile device using both wi- signals as well as cellular wireless standards (e.g. 2G/3G/4G) and (ii) Truconnect Technologies and/or its service partners reserve the right to change how you connect, and stay connected, to Access Point (as de ned in Section 7) through the Truconnect Technologies Software utilizing the Truconnect Technologies Software's proprietary decision making algorithms, which in turn may result in your connection changing to and from wi- and available cellular wireless standards, including, without limitation, roaming onto various carrier networks. When using the Truconnect Technologies Software, you may be subject to, and Truconnect Technologies is not responsible for, your mobile carrier's roaming, access, airtime minutes and surcharges associated with your mobile carrier and applicable data plan. You are solely liable for any applicable carrier charges and must consult your carrier for such information. Truconnect Technologies recommends that you con rm that you have an unlimited mobile-data plan with your mobile carrier before accessing and using the Truconnect Technologies Software.

6. Proprietary Rights - The Truconnect Technologies Software is licensed, not sold. We and our licensors retain exclusive ownership of all worldwide copyrights, trademarks, trade secrets, patents, and all other intellectual property rights (including, but not limited to, any titles, computer code, themes, objects, characters, character names, stories, text, dialog, catch phrases, locations, concepts, artwork, images, photographs, animations, video, sounds, musical compositions, audio-visual effects, methods of operation, moral rights, any related

documentation, and "applets" incorporated into the Truconnect Technologies Software) throughout the world and all applications and registrations therefore, in and to the Truconnect Technologies Software, any full or partial copies thereof, including any additions or modi cations thereto and any accompanying materials, electronic or otherwise. This Agreement grants you no right to use such content other than as part of the Truconnect Technologies Software. The Truconnect Technologies Software is protected by the copyright laws of the United States, international copyright treaties and conventions and other laws. You acknowledge that, except for the limited license rights expressly provided in this Agreement, no right, title, or interest to the intellectual property in the Truconnect Technologies Software is provided to you, and that you do not obtain any rights, express or implied, in the Truconnect

Technologies Software. All rights in and to the Truconnect Technologies Software not expressly granted to you in this Agreement are expressly reserved to us and our licensors. The Truconnect Technologies Software may contain certain licensed materials and Truconnect Technologies' licensors may act to protect their rights in the event of any violation of this Agreement.

7. Sharing of Access Points - When you decide to share an Access Point using the Truconnect Technologies service, you enable other end users of the Truconnect Technologies Software and grant them the right, to access and use such shared Access Point in connection with their use of the Truconnect Technologies Software.

You hereby represent and warrant that (a) you have full authority to grant such access and use rights to any Access Point that you share; (b) your sharing of an Access Point will not breach any agreement or violate any law or regulation or proprietary rights of others, and you agree to defend, indemnify, and hold us, our subsidiaries, af liates, of cers, agents, and other partners and employees, harmless from any loss, liability, claim, or demand, including reasonable attorney's fees, made by any third party due to or arising out of your sharing of an Access Point. An "Access Point" means a computer network device that is used to establish an online connection, such as, but not limited to, a wireless router (Wi-Fi router).

8. Access Points & Network Information - You acknowledge and agree that when you use the Truconnect Technologies Software, Truconnect Technologies may (i) collect information about the computer or mobile device on which the Truconnect Technologies Software is executed and the Access Points that you are using to establish an online connection, including without limitation, the hardware address of its network adapter, the names (SSIDs) of the Access Points, applicable cell network information, location and identi cation of the Access Points, connection status, speed and duration and access control methods; and (ii) collect and store information about the computer or mobile device's data communication session including, without limitation, location based data (GPS pinpoint or cell-ID), time stamps and length of the session and unique user and device identi ers, provided, however, Truconnect Technologies shall not collect or store any information concerning the content of any such communication sessions. By using the Truconnect Technologies Software to connect to any Access Point, you represent and warrant that (i) you have the necessary consent and authority to connect to such Access Point and to permit the sharing of data

related to such Access Points retained by the Truconnect Technologies Software; and (ii) you consent to the terms and conditions for the access and usage of such Access Point required by the owner or provider thereof. Additionally, by using the Truconnect Technologies Software you consent to Truconnect Technologies' analyzing, extracting, compiling and aggregating the data that Truconnect Technologies captures and stores, the results of which shall be solely owned by Truconnect Technologies and may be used by Truconnect Technologies for any lawful business purpose (including, without limitation, providing it to our business partners and third-parties and using it to improve the Truconnect Technologies Software and Truconnect Technologies' service) without additional consent from you, provided that such data is used without speci cally identifying the source. Additional information on how Truconnect Technologies collects, accesses and uses your information is set forth in the privacy policy of TruConnect, which may be viewed at http://www.truconnect.com/legal-privacy-policy (http://www.truconnect.com/legal-privacy-policy), which is speci cally incorporated herein by reference.

9. Disclaimer of Warranties - YOU EXPRESSLY ACKNOWLEDGE AND AGREE THAT USE OF THE TRUCONNECT TECHNOLOGIES SOFTWARE IS AT YOUR SOLE

RISK. THE TRUCONNECT TECHNOLOGIES SOFTWARE IS PROVIDED ON AN "AS IS," "AS AVAILABLE" BASIS, UNLESS SUCH WARRANTIES ARE LEGALLY

INCAPABLE OF EXCLUSION. IN THE EVENT THAT YOU ARE INSTALLING OR USING THE BETA TRUCONNECT TECHNOLOGIES SOFTWARE, YOU FURTHER

ACKNOWLEDGE THAT THE TRUCONNECT TECHNOLOGIES SOFTWARE IS PRE-PRODUCTION AND HAS NOT BEEN COMPLETELY TESTED IN ALL

SITUATIONS. WE PROVIDE NO TECHNICAL SUPPORT, WARRANTIES OR REMEDIES FOR THE BETA TRUCONNECT TECHNOLOGIES SOFTWARE. WE DO NOT

WARRANT THAT THE BETA TRUCONNECT TECHNOLOGIES SOFTWARE IS FREE OF VIRUSES OR OTHER HARMFUL COMPONENTS OR THAT DEFECTS WILL

BE CORRECTED. TRUCONNECT TECHNOLOGIES DOES NOT WARRANT THAT USE OF THE TRUCONNECT TECHNOLOGIES SOFTWARE WILL BE

UNINTERRUPTED, OR ERROR-FREE. TRUCONNECT TECHNOLOGIES AND ITS LICENSORS EXPRESSLY DISCLAIMS ANY AND ALL WARRANTIES AND

CONDITIONS, WHETHER ORAL OR WRITTEN, EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED

WARRANTIES OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT OF THIRD PARTY RIGHTS,

AND THOSE ARISING FROM A COURSE OF DEALING OR USAGE OF TRADE, REGARDING THE TRUCONNECT TECHNOLOGIES SOFTWARE. ANY WARRANTY

AGAINST INFRINGEMENT THAT MAY BE PROVIDED IN SECTION 2-312(3) OF THE UNIFORM COMMERCIAL CODE AND/OR IN ANY OTHER COMPARABLE

STATE STATUTE IS EXPRESSLY DISCLAIMED. TRUCONNECT TECHNOLOGIES AND ITS LICENSORS ASSUME NO RESPONSIBILITY FOR ANY DAMAGES

SUFFERED BY YOU, INCLUDING, BUT NOT LIMITED TO, LOSS OF DATA, ITEMS OR OTHER MATERIALS FROM ERRORS OR OTHER MALFUNCTIONS CAUSED

BY TRUCONNECT TECHNOLOGIES, ITS LICENSORS, LICENSEE AND/OR SUBCONTRACTORS, OR BY YOUR OR ANY OTHER PARTICIPANT'S OWN ERRORS

AND/OR OMISSIONS. YOU ASSUME ALL RISKS ASSOCIATED WITH THE TRUCONNECT TECHNOLOGIES SOFTWARE. WIRELESS INTERNET ACCESS

PRESENTS CHALLENGES FOR PROTECTING YOUR INFORMATION FROM ILLEGAL DATA INTERCEPTION BY THIRD PARTIES. YOU SHOULD CONSULT WITH A

COMPUTER TECHNICIAN TO ENSURE YOUR COMPUTER OR MOBILE DEVICE IS CONFIGURED CORRECTLY FOR SECURE WIRELESS ACCESS TO THE

INTERNET AND THAT YOU HAVE THE LATEST SECURITY SOFTWARE AND HARDWARE INSTALLED. IN NO EVENT WILL TRUCONNECT TECHNOLOGIES BE

OBLIGATED, CONTRACTUALLY OR OTHERWISE, TO INDEMNIFY YOU, OR OTHERWISE REIMBURSE YOU, FOR ANY LOSSES THAT YOU MAY INCUR IN

CONNECTION WITH THE TRUCONNECT TECHNOLOGIES SOFTWARE OR THE SITES YOU MAY VISIT AND PRODUCTS YOU MAY USE WHEN CONNECTED TO AN ACCESS POINT THROUGH THE TRUCONNECT TECHNOLOGIES SOFTWARE. Neither Truconnect Technologies nor its parent, subsidiaries, af liates, licensors and/or its suppliers are responsible for interrupted or unavailable network server or other connections, miscommunications, failed telephone or computer transmissions, or technical failure, jumbled, scrambled or misdirected transmissions, or other errors of any kind whether human, mechanical or electronic or for phone, electrical, network, computer hardware or software program malfunctions, failures or dif culties, or for ISP/network/Web site accessibility or unavailability. You are responsible for assessing your own computer or mobile device, as applicable, and the results to be obtained therefrom. The entire risk arising out of use or performance of the Truconnect Technologies Software remains with you.

10. Limitation of Remedies and Damages - YOU ACKNOWLEDGE AND AGREE THAT TRUCONNECT TECHNOLOGIES, ITS LICENSORS AND SUPPLIERS SHALL

NOT ASSUME OR HAVE ANY LIABILITY FOR ANY ACTION BY TRUCONNECT TECHNOLOGIES, OTHER PARTICIPANTS, OR OTHER LICENSORS WITH RESPECT

TO CONDUCT, COMMUNICATION, OR CONTENT OF THE TRUCONNECT TECHNOLOGIES SOFTWARE. NEITHER WE NOR OUR LICENSORS AND SUPPLIERS

SHALL BE RESPONSIBLE OR LIABLE WITH RESPECT TO ANY SUBJECT MATTER OF THIS AGREEMENT OR TERMS OR CONDITIONS RELATED THERETO

UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER THEORY AND REGARDLESS OF WHETHER SUCH DAMAGES WERE FORESEEABLE OR

COMPANY WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES FOR (A) LOSS OR INACCURACY OF DATA OR COST OF PROCUREMENT OF SUBSTITUTE

GOODS, SERVICES OR TECHNOLOGY; OR (B) ANY INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES INCLUDING, BUT NOT LIMITED TO LOSS OF

REVENUES AND LOSS OF PROFITS. OUR AGGREGATE CUMULATIVE LIABILITY HEREUNDER SHALL NOT EXCEED THE AMOUNTS PAID BY YOU FOR THE TRUCONNECT TECHNOLOGIES SOFTWARE (IF ANY) DURING THE MOST RECENT THREE (3) MONTHS FROM WHEN THE DAMAGE OCCURRED DURING THE TERM OF THE AGREEMENT. CERTAIN STATES AND/OR JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES OR LIMITATION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE EXCLUSIONS SET FORTH ABOVE MAY NOT APPLY TO YOU.

11. Con dentiality - The Beta Truconnect Technologies Software is unannounced and not available to the public. Providing the Beta Truconnect Technologies Software to you does not constitute a sale or an announcement that the Beta Truconnect Technologies Software, or that any other software of a similar design and/or functionality, will be available from us. We consider the Beta Truconnect Technologies Software and any technical information, evaluation or reports supplied to you (the "Con dential Information") to be proprietary, and you agree to not share any Con dential Information with any other third party and not to permit any thirdparty access to the Con dential Information and to take all reasonable steps to secure and protect the Con dential Information from any disclosure or third party access.
12. Feedback - In the event that you provide us with feedback ("Feedback") regarding the use, operation or functionality of the Truconnect Technologies Software, including but not limited to information about operating results, known or suspected bugs, errors or compatibility problems, or desired features, you hereby assign to us all rights in the Feedback. You acknowledge and agree that all Feedback is the sole and exclusive property of Truconnect Technologies and may be used by Truconnect Technologies (or its af liates, publishing partners, distributors, licensors and licensees) for any purpose. If and to the extent you are deemed to have retained, under applicable law, any right, title or interest in or to any portion of your Feedback, you hereby transfer, grant, convey, assign and relinquish solely and exclusively to Truconnect Technologies all of your right, title and interest in and to the Feedback, without reservation and without additional consideration, under applicable patent, copyright, trade secret, trademark and other similar laws or rights, in perpetuity, and in the alternative to the extent such assignment is ineffective under applicable law, you hereby grant to Truconnect Technologies the sole and exclusive, irrevocable, sublicensable, transferable, worldwide, paid-up license to reproduce, x, adapt, modify, translate, reformat, create derivative works from, manufacture, introduce into circulation, publish, distribute, sell, license, sublicense, transfer, rent, lease, transmit, publicly display, publicly perform, provide access to electronically, broadcast, communicate to the public by telecommunication, display, enter into computer memory, and use and practice the Feedback all modi ed and derivative works thereof, all portions and copies thereof in any form, all inventions, designs, and marks embodied therein, and all patent, copyright, trade secret, trademark and other intellectual property rights thereto, or to incorporate the same

in other works in any form, media, or technology now known or later developed. To the extent permitted by applicable laws, you hereby waive any moral rights or rights of publicity or privacy you may have in the Feedback.

13. Consumer End Users Only - The limitations or exclusions of warranties and liability contained in this Agreement do not affect or prejudice the statutory rights of a consumer, i.e., a person acquiring goods otherwise than for use by a business. The limitations or exclusions of warranties and remedies contained in this Agreement shall apply to you only to the extent such limitations or exclusions and remedies are permitted under the laws of the jurisdiction where you are located.

14. Termination - We may terminate this Agreement at any time, with or without cause. You may terminate this Agreement at any time, with or without cause by sending either an e-mail to customercare@truconnect.com with your name and the subject "REMOVE", call 1-800-430-0443, or to such other address as we may specify in writing by posting the new address on the Truconnect Technologies website. Upon expiration or termination, the license granted hereunder shall terminate and you shall immediately destroy any copies of the Truconnect Technologies Software in your possession, including disabling the Truconnect Technologies Software in your device’s setting, but the terms of this Agreement which are intended to survive termination will remain in effect.

15. Modi cations - We reserve the right to change the terms and conditions of this Agreement or our policies relating to the Truconnect Technologies Software at any time, and such changes will be effective upon notice to you. Your continued use of the Truconnect Technologies Software after any such changes shall constitute your consent to such changes.

16. Export - The Truconnect Technologies Software and related technology are subject to U.S. export control laws and may be subject to export or import regulations in other countries. You agree to strictly comply with all such laws and regulations and acknowledge that you have the responsibility to obtain authorization to export, re-export, or import the Truconnect Technologies Software and related technology, as may be required. You will indemnify and hold us harmless from any and all claims, losses, liabilities, damages, nes, penalties, costs and expenses (including attorney's fees) arising from or relating to any breach by you of your obligations under this section. Your obligations under this section shall survive the expiration or termination of this Agreement.

17. Privacy - You agree to the terms of privacy policy that may be viewed at http://www.truconnect.com/legal-privacy-policy (http://www.truconnect.com/legalprivacy-policy).

18. Equitable Remedies - You hereby agree that Truconnect Technologies would be irreparably damaged if the terms of this Agreement were not speci cally enforced, and therefore you agree that Truconnect Technologies shall be entitled, without bond, other security, or proof of damages, to appropriate equitable remedies with respect to breaches of this Agreement, in addition to such other remedies as Truconnect Technologies may otherwise have available to it under applicable laws.

19. Indemnity - You agree to defend, indemnify and hold harmless Truconnect Technologies, its of cers, directors, employees, agents, af liates, successors, assigns, and licensors against and from all damages, losses, liabilities, claims and expenses, including attorneys' fees, arising directly or indirectly from your acts and omissions to act in using the Truconnect Technologies Software pursuant to the terms of this Agreement or any breach of this Agreement by you.

20. U.S. Government Restricted Rights - Truconnect Technologies Software and documentation have been developed entirely at private expense and are provided as "Commercial Computer Software" or "restricted computer software." Use, duplication or disclosure by the U.S. Government or a U.S. Government subcontractor is subject to the restrictions set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clauses in DFARS 252.227-7013 or as set forth in subparagraph (c)(1) and (2) of the Commercial Computer Software Restricted Rights clauses at FAR 52.227-19, as applicable. The Manufacturer is Truconnect Technologies, LLC., 1149 S. Hill St., Suite H-400, Los Angeles, CA 90015, USA.

21. Miscellaneous - You may not use, copy, modify, sublicense, rent, sell, assign or transfer the rights or obligations granted to you in this Agreement, except as expressly provided in this Agreement. Neither the rights nor the obligations arising under this Agreement are assignable by you, and any such attempted assignment or transfer shall be void and without effect. Truconnect Technologies' failure to enforce at any time any of the provisions of this Agreement shall in no way be construed to be a present or future waiver of such provisions, nor in any way affect the right of any party to enforce each and every such provision thereafter. The express waiver by Truconnect Technologies of any provision, condition or requirement of this Agreement shall not constitute a waiver of any future obligation to comply with such provision, condition or requirement. Notwithstanding anything else in this Agreement, no default, delay or failure to perform on the part of Truconnect Technologies shall be considered a breach of this Agreement if such default, delay or failure to perform is shown to be due to causes beyond the reasonable control of Truconnect Technologies. The United Nations Convention on Contracts for the International Sale of Goods shall not apply to this Agreement. In the event that any provision of this Agreement is found to be contrary to law, then such provision shall be construed as nearly as possible to re ect the intention of the parties, with the other provisions remaining in full force and effect. Any notice to you may be provided by e-mail. In the event that any provision of this Agreement shall be held by a court or other tribunal of competent jurisdiction to be unenforceable, such provision will be enforced to the maximum extent permissible and the remaining portions of this Agreement shall remain in full force and effect.

22. Governing Law and Arbitration - This Agreement shall be governed by the laws of the State of Texas without giving effect to any con ict of laws principles that may provide the application of the law of another jurisdiction. Any claim or dispute in connection with this Agreement shall be resolved in a cost-effective manner through binding non-appearance-based arbitration in accordance with the then current Commercial Arbitration Rules of the American Arbitration Association. If you would like more information about the Commercial Arbitration Rules of the American Arbitration Association, please go to

http://www.adr.org/sp.asp?id=22440. The arbitration shall be initiated through an established alternative dispute resolution provider mutually agreed upon by the parties. The arbitrator and the parties must comply with the following rules: a) the arbitration shall be conducted by telephone, online and/or be solely based on written submissions, the speci c manner shall be chosen by the party initiating the arbitration; b) the arbitration shall not involve any personal appearance by the parties or witnesses unless otherwise mutually agreed by the parties; and c) any judgment on the award rendered by the arbitrator may be entered in any court of competent jurisdiction. WE EACH WAIVE ANY RIGHT TO A JURY TRIAL. ARBITRATION INVOLVES A FAIR HEARING BEFORE A NEUTRAL ARBITRATOR RATHER THAN A JUDGE OR JURY. THE ARBITRATOR

MAY AWARD DECLARATORY OR INJUNCTIVE RELIEF ONLY IN FAVOR OF THE INDIVIDUAL PARTY NAMED IN THE ARBITRATION PROCEEDING AND ONLY

TO THE EXTENT NECESSARY TO PROVIDE RELIEF WARRANTED BY THAT PARTY'S INDIVIDUAL CLAIM. THE ARBITRATOR(S) SHALL NOT HAVE THE

AUTHORITY, POWER, OR RIGHT TO ALTER, CHANGE, AMEND, MODIFY, ADD, OR SUBTRACT FROM ANY PROVISION OF THIS AGREEMENT OR TO AWARD PUNITIVE DAMAGES. THE ARBITRATOR SHALL HAVE THE POWER TO ISSUE MANDATORY ORDERS AND RESTRAINING ORDERS IN CONNECTION WITH

THE ARBITRATION. THE AWARD RENDERED BY THE ARBITRATOR SHALL BE FINAL AND BINDING ON THE PARTIES, AND JUDGMENT MAY BE ENTERED

THEREON IN ANY COURT OF COMPETENT JURISDICTION. DURING THE CONTINUANCE OF ANY ARBITRATION PROCEEDING, THE PARTIES SHALL CONTINUE TO PERFORM THEIR RESPECTIVE OBLIGATIONS UNDER THIS AGREEMENT, WHICH ARE NOT AFFECTED BY THE DISPUTE. You agree that

notwithstanding anything to the contrary contained herein, in the event Truconnect Technologies wishes to pursue injunctive or other equitable relief, it may do so in a court of competent jurisdiction in Texas, and you agree to submit to the personal jurisdiction of any such court. This arbitration agreement shall survive the termination of this Agreement. Unless otherwise provided by applicable law, or otherwise in this Agreement, neither party has the right to bring a dispute or other legal action under this Agreement more than one (1) year after the dispute arose.

23. Additional Terms - Your usage of any third-party software or application to navigate to the location of an Access Point identi ed by Truconnect Technologies will be subject to the terms of use of any such third-party software or application. Truconnect Technologies does not warrant, and is not responsible for, the accuracy of any recommendations of Access Point identi ed through Truconnect Technologies including, without limitation, any recommendations with respect to Access Points that are the closest to, or in the vicinity of, you. Additionally, your access and usage of any Access Point identi ed by Truconnect Technologies is subject to all of the terms and conditions required by the owner or provider of such Access Point. Truconnect Technologies is not responsible for the security of any Access Point identi ed by Truconnect Technologies.

24. Entire Agreement - This Agreement, including the relevant terms & conditions found on the TruConnect website, which are hereby incorporated by reference, constitutes the entire agreement between the parties pertaining to the subject matter hereof, and supersedes any and all prior or contemporaneous written or oral agreements between the parties pertaining to the subject matter hereof. To the extent that there is a con ict, this Agreement shall have precedence as to the subject matter of this Agreement.

25. Questions or Additional Information - If you have questions regarding this Agreement, or wish to obtain additional information, please send an e-mail to customercare@truconnect.com or call 1-800-430-0443.

truconnect (http://www.truconnect.com/)

(http://www.facebook.com/TruConnect?ref=hl) (http://twitter.com/TruConnect) (http://www.instagram.com/truconnect_la/) (http://www.truconnect.com/blog/rss-feed/)

WIRELESS

Device (http://www.truconnect.com/english/shop/wireless/wireless-devices.html)

Wireless Plans (http://www.truconnect.com/english/shop/wireless/wireless-plans.html)

LifeLine (http://www.truconnect.com/lifeline/)

Add-Ons (http://www.truconnect.com/international/)

COMPANY

Retail Locations (http://www.truconnect.com/locations/)

Coverage (http://www.truconnect.com/coverage/)

Become a Dealer (http://www.truconnect.com/dealer/)

Dealer Portal (https://dealerportal.truconnect.com/TruConnectDP)

News & Press (http://www.truconnect.com/news-media/)

About us (http://www.truconnect.com/about-us/)

Contact us (http://www.truconnect.com/contact-us/)

Blog (http://www.truconnect.com/blog/)

Careers (http://www.truconnect.com/careers/)

LEGAL

Terms & Conditions (http://www.truconnect.com/legal-terms-and-conditions-personal/)

Privacy Policy (http://www.truconnect.com/legal-privacy-policy/)

Consumer Protection (http://www.truconnect.com/legal-consumer-protection/) Accessibility (http://www.truconnect.com/legal-accessibility/)

Global Texting Countries (http://www.truconnect.com/legal-global-texting/)

Law Enforcement (http://www.truconnect.com/legal-law-enforcement-requests/) Open Internet Statement (http://www.truconnect.com/open-internet-statement/)

What is Lifeline?

Lifeline is a government program that subsidizes discounted phone service for low-income consumers, ensuring everyone can stay in touch. TruConnect is currently designated to provide free Lifeline-supported phone service in numerous states across the U.S., with more coming soon. The Lifeline program is only available to eligible consumers who can provide documentation for eligibility. Only one Lifeline service is allowed per household regardless of type of phone. To be qualified for Lifeline, you must be currently enrolled in a qualified public assistance program (i.e. SNAP, Section 8, LIHEAP, Medicaid/Medi-Cal, NSLP, SSI, WIC, etc.) or you can be qualified if your total annual household income is less than the qualified income guidelines.

Mobile Broadband

TruConnect is a mobile broadband company and a cheap wireless internet provider that offers wireless internet services and mobile WiFi hotspots through Internet on the Go. TruConnect provides an underserved market with prepaid and wireless internet services such as Lifeline (ETC), Wireless Prepaid, and Mobile broadband solutions such as mobile WiFi hotspots. We have a variety of mobile broadband devices ranging from cell phones and 4G smartphones to mobile WiFi hotspot devices and tablets. Our coverage includes a 4G network for nationwide wireless internet.

Why TruConnect?

We are a group of wireless industry veterans who have spent many years bringing new mobile products and services to consumers in the U.S. We understand your frustration with expensive monthly data plans, so we came up with an easy, honest, and convenient way to stay connected to the world with TruConnect Pay As You Go and Lifeline plans, our free text messaging and dialer app (TruText), and with our affordable Internet on the Go mobile broadband plans and hotspots. Individual usage varies from month to month, so we designed our flexible plans to fit your everyday needs. To learn more about Internet on the Go, please visit www.internet-go.com (http://www.internet-go.com). To download the new TruText app, visit www.truconnect.com/get-app (http://www.truconnect.com/get-app).

ANNEX III – Privacy Assessment Audit

Universidad del País Vasco
Euskal Herriko Unibertsitatea

PRIVACY ASSESSMENT OPINION

PRIVACY ASSESSMENT CONCERNING THE WEFI DATASET USED IN THE COGNET PROJECT. OPINION ISSUED BY PROFESSOR ISABEL HERNANDO OF THE BASQUE COUNTRY (UPV/EHU) AT THE REQUEST OF VICOMTECH.

For this purpose, once analyzed the documents (table 1) provided by VICOMTECH, in my opinion and according to the identified documents, the following data protection points seems to have been considered and realized in the CogNet Project :

- Identification of the system of reference: The scope and objectives of the use of the WeFi dataset in the Project, the stakeholders involved in their roles, the assets involved.
- Establishment of the criteria against which the impact of privacy is determined: use of data are minimized for the specific objectives of the CogNet Project and pseudonymized.
- Identification and evaluation of the risks.
- Identification of the levels of risks acceptance.
- Identification of appropriate mitigation strategies: identification of controls and counter-measures.

TABLE 1 . Documents

Nº	Document Identification
1	D1.5. Data Protection and privacy Audit Report
2	8. Access Points & Network Information
3	Wefi – Terms of Service
4	TruConnect Technologies LLC . Order Agreement
5	TruConnect Technologies LLC. Appendix A – Data schema for WeFi Geo-Binned Data – Application and Network Usage Dataset
6	TruConnect Technologies LLC. Appendix B – Data schema for WeFi Network Sessions and QoS Information datasets . WI-FI networks and Cellular networks
7	TruConnect Technologies LLC.. Appendix C – End user License Agreement
8	TruConnect Technologies LLC..Cognet Data Dictionary. Revision 1.1. (10.09.2016)

As a conclusion and in consideration of the information from the above identified documents, I allow myself to express a **POSITIVE OPINION** on the assessment of privacy concerning the WEFI DATASET used in THE COGNET PROJECT.

Opinion issued in Donostia – San Sebastian, on December 15, 2017

Signature: ____________________

Name: Isabel HERNANDO
Title: Professor of Civil Law (UPV/EHU)
Specialized Information Technology Law