DELIVERABLE 2.1
Unity – Legal and Ethical Framework
Executive Summary

Revision 1

Due Date: 31 October 2015
Date of submission: 31 October 2015
Lead Beneficiary of this deliverable: University of Dundee

Dissemination Level: Website/public

Project Title: Unity
Grant Agreement: 653729
Funding Scheme: Research and Innovation action – Safeguarding Secure Society

Duration Time: 36 months
Start date: 01/05/2015

Project funded by the European Commission within the H2020 Framework Programme

Document Summary Information

Authors and Contributors

Initials	Name	Organisation	Role
YH	Yvonne Hail	UoD	WP2 Researcher
MO	Megan O'Neill	UoD	WP2 Lead
DJ	Daniel James	Rini	WP5

Revision History

Revision	Date	Who	Comment

Quality Control

Role	Date	Who	Approved/Comment

Executive summary Legal and Ethical Framework

1. Introduction

The Unity project is a three-year EU Horizon 2020 project with the aim of strengthening engagement and cooperation between police and the diverse communities they serve. Specifically, the project is focused on producing an applied benefit in terms of developing a new communication technology which will sit alongside a newly created community police training programme which are both being developed based on the primary research conducted.

2. Aims and Scope

Given the international scope of Unity and its desire to create locally accountable community policing, in part through the development of relevant technology, an understanding of international and national legal and ethical frameworks is important. The purpose and scope of this report is to outline the legal and ethical frameworks which will structure Unity's work to ensure that it operates at all times in a legally and ethically robust way. The main areas to be considered are the collection, processing, storing and sharing of data and the ethical restrictions on our research into community policing and the operation of the proposed technology to prevent harm to potential research participants and technology users.

The legal framework will take into account European as well as national legislation on data protection. Although all EU member states will be obligated to follow EU law in this area, there is the potential for national legislation to be more restrictive. The inclusion of Macedonia, at present a non-EU state, in this project raises particular issues with regards to any transfer of data into the country. This report will analyse the level of data protection in each participating nation, as well as European law, to arrive at our recommendations for Unity. These recommendations will ensure that Unity is as robust in its data collection, processing, storing and sharing as possible.

An ethical framework is required in order that both researchers and especially the participants taking part in the project can be assured that best practice is being met by the Unity project, thus promoting confidence in the research and ensuring that the findings adhere to the appropriate ethical restrictions. Ethical guidelines are less explicit and uniform than legal requirements, and therefore a wide range of variability is possible across the member states. This report will take the best practice from each partner nation to develop the most robust ethical framework possible. This framework will apply to all aspects of Unity's research as well as to the operation of the technology itself.

3. Unity's technological Components

In order to achieve its vision of enhanced channels of communication to facilitate the sharing of policing priorities for local communities, a mobile application will be developed. This will have one iteration for citizens and one for LEAs. The application will also be supported by a communication portal, as well as requisite data storage facilities. These components will be described in more detail here, in order to guide the analysis of the relevant legal and ethical frameworks to support a robust development and operation of these systems. As the technology described below is in the very early stages of development, what is described here is the current vision. The final version of the applications and portals will depend on the needs of our target community groups (both citizens and LEAs), who have yet to be consulted on this in detail. Thus the technology described here will be subject to change in the future, but the overall legal and ethical requirements will remain constant.

3.1 Citizen Mobile Application

The citizen mobile application will enable the citizen to view reports and crime data as well as provide a portal for the citizen to provide additional information (‘intelligence’) to assist in police investigations and local crime and safety interventions. The citizen will be able to view a certain amount of crime data: there will be aggregate textual reports in each area, complete with various aggregations on local statistics such as type of crime and location.

Using the mobile application, citizens will be able to report a crime, anti-social behaviour or safety issue in the local area, pinpoint where it happened and pass on additional data, in the form of text, audio, video or images so that the police or other LEA will receive this additional evidence and support from the community. The data will be filtered to a degree to ensure that the information is passed to the relevant officer, or resolved quickly (where appropriate) by the staff monitoring the data system.

3.2 Law Enforcement Agency (LEA) Mobile Application

The LEA application will be similar to the citizen mobile application with a slightly different view of the incidents. LEAs will have access to the incident status, with the ability to change, publish or moderate the incidents, based on their permission level via the application. This system will grant officers the ability to update the incident and coordinate activity alongside other LEA officers, as well as the reporters of the incident. As such, access to the application on the LEA side will be very secure and officers must log in to verify that they are able to help through the correct area of responsibility and security clearance.

A feature that allows officers to delegate and coordinate resources within and between LEAs will be implemented as part of the application, allowing officers to monitor the situation as it progresses so they are kept informed. All officers working on the case will have access to the same data.

3.3 Public Community Portal

The public community portal will have similar functionality to the mobile citizen application, although accessible as a website rather than as an ‘app’. This portal will be able to retrieve and display crime data and reports about a local area, and will allow users to access information about specific incidents. Thus the portal gives not only a broad overview of the community crime and other incident data but will be able to look deeper into the individual events which allow more detailed information, which has been moderated and approved, to be viewed publicly. The portal will have integration with social media platforms such as Facebook and Twitter and users of these sites will be able to comment on certain incidents on the portal, allowing easy integration with citizens’ current online activities.

3.4 Private LEA Coordination Portal

The private LEA portal will have similar functionality to the LEA mobile application, using web-based technologies as a portal into the database. The LEA Coordination Portal will act as an answering point, similar to the LEA application, where reports may be built and actioned. The Visualisation Console of the portal includes maps and an overlay of all open incident reports, as well as aggregated reports of crime and other incident data for ease of use.

3.5 Data Driven Analytics Engine

The Data Driven Analytics Engine will take all the information gathered from the mobile applications and the communications portals and correlate information about same incident, identify patterns and generate reports in a way that operators can use to prioritise actions (e.g. the volume of reports per time of crime, a heatmap per geographical location of the reports, risk statistics, etc.). The data collection system will be linked to external data sources to allow better analysis. Results from data analytics are incorporated into rich visualisation forms, which will display neighbourhood incidents (e.g. maps with locations of events, event relations, etc.), risk assessments and support decision-making and allocation of resources. The Analytics Engine data analysis and visual representation techniques will provide real-time data visualization and interaction.

4. Recommendations

The following recommendations for Unity are based on a consideration of the EU Directive 95/46/EC, the incoming changes of the General Data Protection Regulation (GDPR, prosed date of adoption: 2017), the European Convention on Human Rights and the guidelines highlighted through the Delphi Review.

4.1 Recommendations for Unity’s Research

1. All research data collected for Unity should be held in an anonymised format.

2. The partner which collects the data will retain the key for breaking anonymity securely, and will not release this to other partners unless absolutely necessary.

3. All partners in the Unity project will ensure that their data collection and storage systems are highly secure.

4. Should ‘cloud storage’ systems be used, preference should be given to systems based in the EU to ensure that EU level data protection requirements are followed by the cloud storage host.

5. When sending data from one partner nation to another, only very highly secure systems should be used. This is particularly the case when sending data to and from Macedonia, which is not yet a full member of the EU.

6. All participants in Unity’s research will be asked to give informed consent to participate in the project. This consent should be in writing.

7. All participants in Unity’s research will be notified about the retention period of their data, the purposes for which their data will be used, their right to withdraw their participation and their data at any time and that their participation is entirely

voluntary. This latter point will be a particular issue for LEA participants, who may be asked to participate in research by a superior officer.
8. Children and vulnerable persons should not be included in Unity's research, due to the more complicated processes of obtaining their informed consent.

9. Participants in Unity's research should have access to the findings from this work, such as research publications or briefing papers. These will be made available, subject to any copyright restrictions, on the Unity Project webpage.

4.2 Recommendations for Unity's Mobile Applications ('Apps') and Portals

1. All data collected through the Unity app and portals are only to be used for the stated purposes.

2. Only data which is absolutely necessary for the functioning of the app and portal are to be collected.
3. All data collected, stored, processed and retrieved by the Unity app, portals, databases and authorised users will be held and transferred through highly secure systems to prevent loss, damage or unauthorised access. These systems should not be based outside the EU unless absolutely necessary.

4. In order to be assured of a secure connection to the app and portal, only staff present on-site in LEA offices should be able to log on to the system. No home working use should be allowed.

5. Users of the app and portal will be made aware of the limitations of these services, the extent of data to be collected (including their IP address), their right to remain anonymous and the purposes for which this information will used.

6. Users of the app and portal will be given the ability to opt out of the collection of personal and sensitive data about him or her, including their IP address. This should be given in a clear and concise manner suited to the small screen so that users can give their full consent to the data which is collected about them and the reasons why it is being requested. Users should not feel pressured to supply personal or sensitive information that they do not wish to share.

7. Users will be notified of the parties to whom the data may be transferred, the conditions for transferring the data to third parties, and the rights of the individual (data subject) concerning further processing of their personal data.

8. Users should be given the contact details for the data controller and processors and the retention period of their data.

9. Users will have the right to access the personal data held in relation to them in the Unity databases and the right to rectify it, if need be.

10. LEAs should check with their national regulatory authority as to whether they need to register as a data controller/exporter prior to the processing of data. This is especially the case for LEAs in Belgium, Bulgaria and Croatia.

11. The app and portals will use encryption services to ensure the secure transfer of data from the app and portals to the LEAs and from the LEAs to other partner agencies, either within that country or outside of it.

12. A Privacy Impact Assessment would be good practice for the app and portals.

13. Crime maps must be designed in such a way that no particular home or address can be identified from a crime or other incident reported on it. This includes cases of multiple crimes/events and uploading events in ‘real time’.

14. In addition, linking events in the crime maps to social media platforms (like Facebook and Twitter) will introduce the possibility of cross-linking of information which could render an individual identifiable. This needs to be avoided.

15. Users should have a right to change their mind and withdraw any personal data which is sent.

16. The app and portals should not be used by children or vulnerable persons, and should be designed in such a way so as to discourage their use by these populations if at all possible.

17. Images, voice recordings and video can be classed as personal data and need to be held as securely as other forms of personal data. This is especially the case if the image or voice of an individual who has not consented to using the Unity app or portal is inadvertently captured by a consenting user. In these cases, very careful consideration should be given before these materials are released on the public portal or app.

18. Images and video of children can have particular data protection issues and should be reviewed carefully before being made public.

19. Should the LEA app and private portal be accessible on portable devices (smart phones, tablets, etc.) these need to be equipped with robust security systems to prevent the data being accessed by unauthorised individuals should the devices be lost or stolen.

20. Publication of a crime or other incident on the public portal and app should be decided on a case-by-case basis to ensure that no person’s privacy is violated. All information published about an incident should be anonymised.

5. Conclusion

The summary above has set the legal and ethical framework which will underpin the work of Unity. This framework includes both the research process and the technical outputs which will be developed from the findings of the research. Providing a framework as set out above, ensures that work conducted by the Unity partners is at all times legally and ethically robust. The legal framework takes into account European as well as national legislation on data protection.