D3.1 Initial Report on Compliance with Ethical Principles

Grant Agreement:	833635
Project Acronym:	ROXANNE
Project Title:	Real time network, text, and speaker analytics for combating organised crime
Call ID: **Call name:**	H2020-SU-SEC-2018-2019-2020, Technologies to enhance the fight against crime and terrorism
Revision:	V1.0
Date:	02 November 2020
Due date:	01 November 2020 (Delayed from 1 September 2020)
Deliverable lead:	TRI
Work package:	WP3
Type of action:	RIA

Disclaimer

The information, documentation and figures available in this deliverable are written by the “ROXANNE - Real time network, text, and speaker analytics for combating organised crime” project’s consortium under EC grant agreement 8833635 and do not necessarily reflect the views of the European Commission.

The European Commission is not liable for any use that may be made of the information contained herein.

Copyright notice

Project co-funded by the European Commission within the H2020 Programme (2014-2020)		
Nature of deliverable:	R	
Dissemination Level		
PU	Public	☒
CO	Confidential, only for members of the consortium (including the Commission Services)	□
EU-RES	Classified Information: RESTREINT UE (Commission Decision 2015/444/EC)	□
* R: Document, report (excluding the periodic and final reports) DEM: Demonstrator, pilot, prototype, plan designs DEC: Websites, patents filing, press & media actions, videos, etc. OTHER: Software, technical diagram, etc.		

Revision history

Revision	Edition date	Author	Modified Sections / Pages	Comments
V0.1	21 Oct 2019	David Wright (TRI)		Original draft
V0.2	2 Dec 2019	David Wright (TRI)		
V0.3	10 July 2020	Joshua Hughes (TRI), David Barnard-Wills (TRI), Shivam Garg (CAPGEMINI), Xenia Burlaca (INTERPOL)		
V0.4	22 July 2020	INTEPROL (John Barry & Xenia Burlaca)	Review and addition of recommendations	
V0.5	11 August 2020	David Barnard-Wills(TRI)		Review
V0.6	9 October 2020	Joshua Hughes (TRI)	All	
V0.7	22 October 2020	Joshua Hughes (TRI)	All	
V0.8	28th October 2020	Shivam Garg (CAP)	All	
V0.9	29 October 2020	Stela Lipcan (INT)		
V0.10	30 October 2020	Joshua Hughes (TRI)	All	Review and edits
v1.0	31 October 2020	Petr Motlicek (Idiap)	All	proof-reading

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

Executive summary

This initial assessment of ethics, societal values, fundamental rights, and applicable legislation describes potential risks that could arise for the project in each of these areas. It also provides suggestions of how the project partners and, in some cases end-users, could mitigate or avoid these risks. First, this deliverable outlines the nature of the ROXANNE Ethics Boards and how they discuss issues and contribute ethical oversight to the project. Then, the function and use of the ROXANNE ethics touchpoint table is described; this is a new tool for ethical analysis that has been implemented in the ROXANNE project by WP3 partners and was used as a starting point for the more detailed analysis provided in this document. Next, the key ethical concepts that have been used to analyse the project are discussed. The detailed analysis of the project according to each ethical concept across 6 phases is then provided.

In terms of societal values, a description of the process used for analysing different values is then provided and this is followed by a briefing paper that will be disseminated to different stakeholders; this document analyses several societal values for their relevance to the project and use of the platform, issues that could occur and mitigation measures. A description of stakeholders whom the document will be sent to is also provided. Finally, two scenarios that will be distributed in order to generate discussion and feedback from stakeholders are included.

With regard to fundamental rights, first it is explained that WP3 partners took business and human rights, and comparative approaches in order to analyse issues present in both the ROXANNE project and potential use of the platform. Then, fundamental rights that are relevant to ROXANNE are described in terms of both the project and potential use of the platform, and the issues generated for them are detailed and discussed; measures to mitigate these impacts are also provided. Finally, two scenarios that will be used as discussion documents with stakeholders, and to gather feedback, are provided.

In terms of applicable legislation, the way in which partners conducted the research is explained, as is the different pieces of legislation and specific areas that were focussed on. Next, the analysis is provided as a checklist, which will be given to partners in order to ensure that their data-processing operations are in compliance with legal rules. Then a description of the members, and operation, of the Security Advisory Board is given.

Finally, emerging themes that have arisen across the analysis of the different analytical areas are presented, and those that need further research are noted. Then, an explanation of the work to be done in WP3 in the future is provided, before concluding. The annexes include a list of every requirement generated by the analysis, and the ethics touchpoint table used by WP3 partners is also provided.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635.

Table of contents

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

1. Introduction

1.1. Background

ROXANNE WP3 concerns compliance with ethical principles, EU societal values, fundamental rights and legislation. The key partners are TRI, CAPGEMINI, INTERPOL, KEMEA and AIRBUS. WP3 has several tasks, of which this deliverable responds to four, namely:

- T3.1: Adhere to good ethical practices
    - ST3.1.1.: Logistics
    - ST3.1.2.: Identify and assess ethical issues arising from the project
- T3.2: Comply with societal values
- T3.3: Comply with fundamental rights
- T3.4: Comply with applicable legislation, including in the area of free movement of persons, privacy and protection of personal data

ST3.1.1 Logistics involves setting up and running the project's Ethics Board. Following the funding of the project, the European Commission added ethics requirements to the proposal to WP10. Several deliverables in that work package include information on the ROXANNE Internal and External Ethics Boards. At the time of writing, two of these deliverables have been submitted, D10.12 and D10.13. D10.12 includes information about the nature of the ethics boards, their memberships, how they function, a draft agenda, and terms of reference along with a recommendation that members of ethics boards who are external to the project should be remunerated for their work. For D10.13, the consortium was asked to provide a report by the External Ethics Board (EEB). Owing to nature of EEB members serving in their spare time, the consortium has sought to reduce the time they spend on this report. Previous versions of this deliverable included a report drafted by consortium members and approved by EEB members, and a record of meetings. Neither were deemed by the EC to be a report by the EEB, and so EEB members are currently writing a report for the consortium. Consequently, as detailed information about the ethics boards in ROXANNE has already been provided, it will not be repeated here. However, additional information on the process for setting the Ethics Board up is included.

1.2. Purpose and scope

The purpose of this deliverable is to respond to the first four tasks in WP3. Those tasks are:

T3.1 Adhere to good ethical practices

> ST 3.1.1 – Logistics: TRI will establish an ethics board (see section 3.2, Grant Agreement). The partners will compile a list of the titles and contact details of the national ethics committees in the countries of the partners or the partner institution's own ethics committee. In other instances, TRI will form a project ethics board. The partners will prepare informed consent for use in interviews and workshops. TRI will ensure that partners obtain and keep on file the opinions or approvals by ethics committees and/or competent authorities.
>
> ST 3.1.2 – Identify and assess ethical issues arising from the project: The partners will compile a list of all the activities to be undertaken and will identify and assess any ethical issues that might arise from each of those. The partners will discuss with the WP leader what measures could be taken to address the ethical issues proposing solutions and future steps.

T3.2 Comply with societal values

CAP and TRI will conduct a literature review on societal values and draft a workshop briefing paper. A workshop with external AB members will be convened (i.e. end-user workshop organized at KEMEA in M9) to discuss (a) how the project will address societal values and (b) what measures can be taken to avoid any harm to societal values. The partners will create a series of brief scenarios (vignettes) featuring different societal values (as the perception of security, possible side effects of technological solutions and societal resilience) and how the project will address them, post them on the project website and invite reactions from citizens.

T3.3 Comply with fundamental rights

The partners will prepare an analysis about what and how fundamental rights might be impacted by the project's proposed solutions. The partners' analysis will be based on selected rights from the Charter of Fundamental Rights of EU. The analysis will provide several examples, like the vignettes in the previous task. The partners will disseminate the analysis to LEAs exploiting INTERPOL's global LEA network, policymakers, and civil society organizations.

T3.4 Comply with applicable legislation, including in the area of free movement of persons, privacy and protection of personal data

The partners will create digital brochure containing a checklist of the relevant provisions of applicable legislation such as the GDPR, the INTERPOL Rules on the Processing of Data, the Police Directive, the Network and Information Security Directive, etc., how partners and stakeholders can comply with the relevant provisions (update in M36). T3.4 will nominate security advisory board (see Section 6.3.2, Grant Agreement).

1.3. Document structure

This deliverable is in four parts, each of which responds to a relevant task in numerical order. Section 2 provides results of T3.1. Section 3 explains the analysis of social values form T3.2. Section 4 displays the evaluation of fundamental rights from T3.3. Section 5 show the assessment of applicable legislation from T3.4. Section 6 outlines some overarching themes from the ethics, societal, and legal analyses. Section 7 explains how work on ethical, societal, and legal issues will continue in the rest of the project, and Section 8 concludes the document.

In Annex A, a table collating all of the requirements from the document is provided. In Annex B, a record of the Ethics touchpoint table used for initial ethical analysis is provided.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

2. T3.1 Adhere to good ethical practices

This section contains two subsections. The first explains that the development of the ROXANNE Ethics Board follows EC guidance. The second provides an explanation of the process, and the results of the analysis of the ethical analysis of the ROXANNE project and platform.

2.1. ST 3.1.1 – Logistics

The Ethics Sector of the EC DG Research and Innovation formed a Working Group to provide guidance on the roles and operation of ethics advisors (EAs) and ethics advisory boards (EABs) to monitor, guide and counsel EC-funded projects.[1] The Working Group produced a 20-page guidance document in 2012. This appears to be the most recent document addressing EAs and EABs. The ROXANNE partners used this guidance to inform the development of the ROXANNE Ethics Board. At this point it is worth reiterating that, following a recommendation from external members of the ROXANNE Ethics Board, the project separated members into Internal and External Ethics Boards. Details of the composition and terms of reference of the ROXANNE Internal and External Ethics Boards are provided in D10.12 (M1), and reports of the External Ethics Board are found in D10.13 (M4), D10.14 (M12, delayed), and D10.15 (M30).

There are several points to note about this document:

- It was produced by a Working Group appointed by the European Commission. The document is not official EC policy. Indeed, its status is not quite clear. It is not clear whether the European Commission accepts all of the recommendations, suggestions and guidance in the document.
- For an ethics board to perform all of the functions mentioned in the document would take quite a lot of time, far more than can reasonably be asked of a volunteer Ethics Board. It is not realistic to assume that senior ethicists would be willing to do so much work free of charge.
- Internal members of the ROXANNE Ethics Board reviewed the document and noted various points (see below). ROXANNE project partners provide comment on some of the points from the guidance document below.

In the table below we cite some relevant provisions from the Working Group document and by our comment.

Working Group provisions	Our comment
Membership should cover expertise in law, data protection/privacy and research ethics and substantive experience in the assessment of ethics issues in the specific topic area of the project.[2]	The ROXANNE Internal and External Ethics Boards are multidisciplinary and have expertise in all of these areas. Members of both ROXANNE ethics boards have diverse experience and expertise relevant to the ROXANNE project, as noted in D10.12.
The EAB … comprises partners and 'non-partner'/independent experts who 'work together' in the best interests of the overall project.[3]	The ROXANNE Ethics Board, as originally devised, comprised four members external to the consortium and four partner representatives. Having been separated, the Internal Ethics Board includes 14 members from across the consortium. The External Ethics Board includes five members

[1] European Commission, DG Research and Innovation, Roles and Functions of Ethics Advisors/Ethics Advisory Boards in EC-funded Projects, December 2012 (hereafter: EC, December 2012), p. 1. https://ec.europa.eu/research/participants/data/ref/h2020/other/hi/ethics-guide-advisors_en.pdf

[2] EC, December 2012, p. 3.

[3] EC, December 2012, p. 4.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635.

	from ethics, law, and technology.
An EAB Chairperson should be elected from the membership and may speak on their behalf. [4]	As noted in D10.13 (v2.0), the ROXANNE partners have expressed a preference for a rotating chair in External Ethics Board meetings, and for the Chairperson to always be an external member.
It should be clearly outlined in a Memorandum of Understanding (MOU) how the interaction between the consortium and the Ethics Advisory Board takes place and the mandate of the EAB ... should be clearly defined. [5]	While we do not see the need for a formal MoU, the consortium has created a terms of reference document that describes the interactions expected between the consortium and the External Ethics Board. This is found in D10.12.
Ethical issues can become quite formidable or can be capable of being addressed in a straightforward way – largely dependent on the primary substantive focus of the project. In all cases 'proportionality' is of the utmost importance. EA/EAB practice should be proportionate to the topic in hand. The format and frequency of meetings should reflect this proportionality, as should the reporting function. Project partners should be invited to meetings in case specific questions need to be addressed. [6]	The ROXANNE consortium believes it has struck the right balance – the right proportionality – between the research and the ethical considerations relating to that research. We have several "gates" on ethical considerations. First, the ROXANNE ethics and data protection advisor (TRI) considers the various tasks in the project and identifies possible ethical and/or data protection issues that might arise in each of the various tasks. Second, the task leader considers the various issues identified by TRI and whether he or she agrees with those issues or whether they see some other issues not identified by TRI. Third, TRI will raise consideration of those various issues with the Internal and External Ethics Boards to have their views and to see whether they see some other issues still.
EAs/EABs exist to offer guidance, advice, monitoring and recommendations for future work. Boards and advisors should operate according to the mandate outlined in the MOU at the beginning of the project – neither dominating the work nor obstructing it unnecessarily. [7]	Agreed!
Funding must be adequate to the task. Clarity over fees and expenses is vital. The workload in complicated projects can be very high and may require the commitment of several full days per year…. ***compensation for the work should be foreseen in the project application***. [Boldface added.] *To avoid conflicts of interests and compromising its independence as a result of financial interests, the compensation budget should not be linked to any specific outcome of the ethical assessments. Since members are acting in an advisory capacity, it is hard to fully anticipate the budget in advance since the need to address unanticipated issues might occur. This suggests that some room for manoeuvre within the budget is*	Although the ROXANNE budget does not contain a provision for paying for EB members' time, it does cover the cost of their travel to one face-to-face meeting a year. However, as we indicated in D10.12, we recommend in future that budgetary provision is made for EB members' time, as we estimate that each member would consume at least 7 days a year to meet the responsibilities of the ethics board. We agree with the Working Group recommendation which we have highlighted in boldface (left). It should be noted that, due to difficulties of EEB members finding spare time to write their reports voluntarily, the consortium has opted to pay EEB members for their time to write the reports D10.13

[4] EC, December 2012, p. 4.

[5] EC, December 2012, p. 5.

[6] EC, December 2012, p. 5.

[7] EC, December 2012, p. 5.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

needed. There must also be clarity over who and what is to be paid for and what activities are "voluntary" in order to ensure members are treated equitably.[8]	and D10.14. This is being done out of partners pre-existing budgets.
Face-to-face… meetings should take place as often as possible to ensure active discussions between the members of the EAB and also with the researchers involved in the project.[9]	ROXANNE envisages one face-to-face meeting a year, which we think is proportionate to the needs of the project. In addition, we are planning for at least three conference calls per year. Owing to the ongoing Coronavirus pandemic, all meetings have been virtual so far.
The individual members of the EAB should cooperate to work out consensus-based recommendations. In cases where no consensus can be reached, it is recommended that the EAB provide a transparent overview on its discussion to the project management, detailing why no definitive advice was possible.[10]	Agreed! As noted in D10.12, the ROXANNE consortium would prefer its ethics boards to make decisions by consensus, but would accept majority decisions where consensus is not possible.
All meetings of the EAB should be based on an agreed agenda to ensure efficient decision-making. Relevant documents should be circulated beforehand to allow for adequate preparation. Meetings should be co-ordinated by the Chairperson and a report should be prepared for each meeting and communicated to the project management.[11]	Agreed!
EAs/EABs are resources for advice and guidance when ethical dilemmas arise during a project.[12]	Agreed!
The EA/EAB Chair should be ex officio a member of the AB.[13]	Owing to the External Ethics Board having a rotating Chairperson, it is not fair to invite only one member of this Board. Consequently, major issues that are discussed with the Stakeholder Board will also be brought to the External Ethics Board where necessary.
The work of EABs can produce judgements that may conflict with project goals. Therefore, much higher emphasis must be given to ensuring independence and limiting conflicts of interest in such circumstances.[14]	This is a risk. However, the consortium partners will explain clearly what we are doing, but even after doing so, the External Ethics Board may have a different view. If so, the project management committee and/or the project co-ordinator will decide whether to comply with the EB advice.
Transparency and critical detachment are important components of ethical oversight. Being open and clear about decisions, actions to take and the rationales behind them is good practice.	Agreed!

[8] EC, December 2012, p. 5.
[9] EC, December 2012, pp. 5-6.
[10] EC, December 2012, p. 6.
[11] EC, December 2012, p. 6.
[12] EC, December 2012, p. 6.
[13] EC, December 2012, p. 6.
[14] EC, December 2012, p. 8.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

All other project groups (partners and advisors) should be encouraged to raise issues with the EA/EAB knowing they are to be treated with discretion. [15]	
The EA/EAB should do whatever is necessary to diligently monitor the aims, objectives, methodology and implications of the research to ensure that it conforms to the highest ethical standards and ensures that the researchers, the Commission and the general public are not exposed, by the work of the project, to activities that would be considered to be ethically unacceptable.[16]	Yes, with the provision that ethics board members' time is limited.

Conclusions from review of the prescriptions for project ethics boards

While the 2012 recommendations from an independent working group contain much to consider, we make a few important observations. As an EC document, we can assume that it has been endorsed by the EC. Although the guidance is eight years old, it is still referred to in other EC documents, and so we can assume the advice is still current.[17]

Further, and most importantly, the working group makes recommendations for the activities of ethics boards that would consume a lot of time for voluntary and unpaid members of the External Ethics Board. We generally think ethics board members who are requested by the EC to write reports should be remunerated for their time, the requirement for them to write reports was not foreseen before the imposition of the WP10 requirements and so no such provision exists in the project budget. Consequently, the EEB members are being paid for their time form partner's budgets. Even so, the ROXANNE consortium believes that the EC, and other consortia, should recognise that most ethics board members will be constrained by the amount of time they can devote to projects.

Finally, the working group does make statements, observations and recommendations with which we agree. So, while we cannot implement all of the recommendations, nevertheless, we find it to be a useful reference.

2.2. ST 3.1.2 – Identify and assess ethical issues arising from the project

There are (at least) four stages or gates through which we pass in our identification of ethics issues.

First, TRI has prepared an ethics touchpoint table (see below) that makes an initial identification of ethics issues, task by task.

Second, TRI initiated discussion with each of the WP leaders to see whether they agree with the findings or wish to amend the touchpoint table.

[15] EC, December 2012, p. 8.

[16] EC, December 2012, p. 8.

[17] European Commission, DG for Research & Innovation, How to complete your ethics self-assessment, February 2019, pp.40-41. Available at: https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-self-assess_en.pdf

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

Third, TRI sent the amended touchpoint table to the ethics board members, for its consideration and discussion. (Owing to the need to discuss WP10 deliverables at length, detailed discussion of the touchpoint table with the EEB has not be as extensive as initially envisaged.

Fourth, following discussion with the ethics board, WP3 partners use the touchpoint table as an initial basis for forming ethical/societal/legal requirements and recommendations for the project..

It is relatively easy to construct an ethics touchpoint table. It consists of four columns: the first is the title or summary of each task in the project. The second lists the ethical, data protection and societal issues that the ethics advisor sees prospectively. The third column are the ways of addressing the issues. The fourth column provides an assessment of the risk. The table provides structured and useful means for discussing the ethical, data protection and societal issues arising in each task with the task leaders and the ethics board. The ethics touchpoint table is included below in Annex A. An example excerpt from the ethics touchpoint table is provided below:

Task	Task description	Potential Ethical issues	Addressing these issues	Assessment of risk
…				
T2.1 Collection of End-User Requirements	Besides NFI and other LEAs, the project will involve a wide group of end-users (stakeholders): LEA experts worldwide, through the INTERPOL's global law enforcement network. In order to collect end-user requirements from these stakeholders, NFI will prepare a global survey, validated by ROXANNE partners. This survey will be communicated through INTERPOL's network (192 member countries) of National Central Bureaus (NCBs) and also completed by members of external Advisory Board (AB) and will be communicated at the end-user meeting organized at 1st field-test (M9). NFI and INTERPOL will create a group of project stakeholders to be invited to attend 2nd (M20) and 3rd field-test (M30) meetings (separate budget reserved through ROXANNE coordinator, see Table 3.4b at page 70). The goal is to collect additional feedback and new knowledge in the project's field. This process will include direct interaction with LEA officials working under operational conditions.	Privacy and Data governance issues regarding personal data in responses to the survey. Diversity, non-discrimination and fairness issues in terms of selecting members of the Stakeholder Board.	The partners will collect end-user requirements taking into account privacy and data governance standards in particular. We will anonymise individuals, if they are mentioned at all in survey responses. The survey responses will be diverse, due to being distributed through INTERPOL's global communications network. We will ensure a balance of participants in the Stakeholder Board according to gender, geographical, and cultural background.	Low

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

…

The ethics touchpoint table should be a living document, i.e., it should be amended as the tasks are undertaken and completed.

The key component of the ethics touchpoint table is the list of ethics principles to which one can refer in reviewing the project tasks. That is the subject of the next section.

Ethics principles

There are many sets of ethics principles. The EU-funded SHERPA project, which is focused on the ethics of artificial intelligence, found over 70 such codes.[18] The project developed a set of criteria for determining which codes should be examined in more detail. It created a "short" list of 25 codes of ethics that met the criteria set by the project. The short list included many important guidelines, such as those of the Organisation for Economic Co-operation and Development (OECD); the EC High-Level Expert Group on Artificial Intelligence (AI HLEG); and the Global Initiative on Ethics of Autonomous and Intelligent Systems from the Institute of Electrical and Electronics Engineers (IEEE).

As the HLEG guidelines were prepared for the EU and are quite detailed, and because SHERPA gave a qualified endorsement to many of the first HLEG report findings, SHERPA adopted the HLEG's seven principal requirements as its baseline. However, SHERPA did not adopt the HLEG principles in their entirety and without modification. Rather, SHERPA adapted them, in part by additions and inputs and tweaks from the other 24 sets of guidelines it examined in detail. In effect, SHERPA took the best of all of them. This was not unduly complicated, as the researchers found a high degree of consonance between the various codes.

As the SHERPA ethical requirements represent a consolidated set, ROXANNE has adopted or adapted them as the source for the ethics guidelines governing our project.

Each of the seven SHERPA ethical requirements is subdivided into subsets of subsidiary or associated principles. The following table lists the seven ethical requirements as well as the subsidiary principles associated with each of the main guidelines.

SHERPA requirements and sub-requirements
1 Human agency, liberty and dignity: Positive liberty, negative liberty and human dignity
2 Technical robustness and safety: Including resilience to attack and security, fall back plan and general safety, accuracy, reliability and reproducibility

[18] Philip Brey, Björn Lundgren, Kevin Macnish, and Mark Ryan, 'D3.2 Guidelines for the development and use of SIS', SHERPA project, 2019, p.10 (hereafter: 'SHERPA Guidelines'). Available at: https://dmu.figshare.com/articles/D3_2_Guidelines_for_the_development_and_the_use_of_SIS/11316833

3 Privacy and data governance: Including respect for privacy, quality and integrity of data, access to data, data rights and ownership
4 Transparency: Including traceability, explainability and communication
5 Diversity, non-discrimination and fairness: Avoidance and reduction of bias, ensuring fairness and avoidance of discrimination, and inclusive stakeholder engagement
6 Individual, societal and environmental wellbeing: Sustainable and environmentally friendly smart information systems, individual well-being, social relationships and social cohesion, and democracy and strong institutions
7 Accountability: Auditability, minimisation and reporting of negative impact, internal and external governance frameworks, redress, and human oversight

These ethical requirements come from SHERPA deliverable D3.2 (Guidelines for the development and use of SIS).[19] Each of the guidelines is spelled out in some detail and often referring to source material, namely, the 25 sets of ethical guidelines it reviewed in detail. A brief overview of each ethical requirement and their implications for ROXANNE is now provided.

Human agency, liberty, and dignity

The first SHERPA high-level requirement includes the following sub-requirements: '*Positive liberty, negative liberty and human dignity*.'[20] This is explained as being important:

> '*Because we value the ability for humans to be autonomous and self-governing (positive liberty), humans' freedom from external restrictions (negative liberties, such as freedom of movement or freedom of association), and because we hold that each individual has an inherent worth and that we should not undermine the respect for human life (human dignity), we need to ensure that AI and big data systems do not negatively affect human agency, liberty, and dignity*.'[21]

Throughout each phase, the ethical risks presented under this requirement could manifest so that persons will not have their agency and liberty respected, or will not be treated in a dignified manner. Human agency as an ethical concept is fundamentally about individual people having agency over their lives. It has a clear link to positive liberty, i.e. the ability for human beings to be autonomous and self-governing. It also connects to concepts of dignity and whether human beings are being treated in a dignified way.[22]

Technical robustness and safety

This requirement includes the following sub-requirements: '*resilience to attack and security, fall back plan and general safety, accuracy, reliability and reproducibility*.'[23]

This is explained as:

[19] SHERPA Guidelines, p.1

[20] SHERPA Guidelines, p.13

[21] SHERPA Guidelines, p.13

[22] Griffin, James, *On Human Rights*, OUP, Oxford, 2008, pp.44-48.

[23] SHERPA Guidelines, p.12

> ‘*Because we value humans, human life, and human resources, it is important that the system and its use is safe (often defined as an absence of risk) and secure (often defined as a protection against harm, i.e., something which achieves safety). Under this category we also include the quality of system decisions in terms of their accuracy, reliability, and precision.*’

Consequently, the aim of implementing this requirement is to ensure that work on the ROXANNE project, and the ROXANNE platform is safe, secure, accurate, reliable, and precise.

Privacy and data governance

The ethical requirement of privacy data governance includes the following sub-requirements: ‘*Including respect for privacy, quality and integrity of data, access to data, data rights and ownership*.’

This is explained in the following way:

> *‘Because AI and big data systems often use information or data that is private or sensitive, it is important to make sure that the system does not violate or infringe upon the right to privacy, and that private and sensitive data is well-protected. While the definition of privacy and the right to privacy is controversial, it is closely linked to the importance of an individual's ability to have a private life, which is a human right. Under this requirement we also include issues relating to quality and integrity of data (i.e., whether the data is representative of reality), and access to data, as well as other data rights such as ownership.’*

Fundamentally, the ROXANNE platform is a collection of data processing tools: data is inputted and analysed, and results are outputted. During its use, most, if not all, of these data will be personal data from LEA investigations.[24] As such, the use of the platform must conform to the EU Law Enforcement Directive that regulates the processing of personal data for law enforcement purposes, and the research and development of the tools needs to be in compliance with the General Data Protection Regulation that governs the processing of personal data in other circumstances.

The major legal issues generated by complying with these two pieces of legislation are detailed below (Section 5 (T3.4, Comply with Applicable legislation)), this section focuses on the ethical issues of processing personal data. Of course, there are areas where ethical and legal concerns cross-over.

Transparency

The ethical requirement for transparency includes the following sub-requirements: ‘*traceability, explainability and communication’*.[25]

These are important:

> *‘Because AI and big data systems can be involved in high-stakes decision-making, it is important to understand how the system achieves its decisions. Transparency, and concepts such as explainability, explicability, and traceability relate to the importance of having (or being able to gain) information about a system (transparency), and being able to understand or explain a system and why it behaves as it does (explainability).’*[26]

[24] Art.4(1), European Parliament and Council, Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, OJ L 119, Vol.59, 4 May 2016 (General Data Protection Regulation, hereafter: GDPR)

[25] SHERPA Guidelines, p.12.

[26] SHERPA Guidelines, p.13.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

Transparency can be defined as '*the quality of being done in an open way without secrets*'[27]. Transparency is one of the most important ethical factors while trying to analyse ethical issues since it is one of the pre-requisites for trust.

The lack of adequate transparency and public accountability mechanisms throughout the process of the design, development and implementation of data-analysis platforms, such as ROXANNE, that are intended to be used by LEAs are an area of concern. There is still inadequate information, and insufficient public discussion on: the actual operation of these technologies and the conditions required for a successful use; the possible consequences; the quality and "credentials" of the various actors involved; the ways it would be applied and in what contexts and who should be held accountable for this. Transparency and information about the development of new security technologies is also crucial if we are to foster trust, so it is important to take inputs from public on a project such as the ROXANNE. Additionally, as ROXANNE is a new and highly-complex technology, It is important to understand how the system works, this is known as 'algorithmic transparency', and this is discussed in the detailed analysis below.

Diversity, non-discrimination and fairness

The SHERPA ethical guidelines supplement the high-level requirements of diversity, non-discrimination and fairness with the sub-requirements of "*avoidance and reduction of bias, ensuring fairness and avoidance of discrimination, and inclusive stakeholder engagement*"[28] further explaining associated risks in case of non-compliance:

> "*Because bias can be found at all levels of the AI and big data systems (datasets, algorithms, or users' interpretation), it is vital that this is identified and removed. Systems should be developed with an inclusionary, fair, and non-discriminatory agenda. Including people from diverse backgrounds (e.g., different ethnicities, genders, disabilities, ideologies, and belief systems), stakeholder engagement, and diversity analysis reports and product testing, are ways to include diverse views into these systems*."[29]

Diversity in all its forms is important for the ROXANNE project so as to ensure that the policies, processes, and activities of the consortium respect contributions from the broadest possible group of researchers and stakeholders. It is also particularly important to the development and use of the ROXANNE platform to ensure that the results of the data analysis are not skewed by biased data.

Individual, Societal, and Environmental Wellbeing

This requirement has the following sub-requirements: '*Sustainable and environmentally friendly AI and big data systems, individual wellbeing, social relationships and social cohesion, and democracy and strong institutions*.'

It is explained as:

> '*Because AI and big data systems can have huge effects for individuals, society, and the environment, systems should be trialled, tested, and anomaly-detected, to ensure the reduction, elimination, and reversal of harm caused to individual, societal and environmental wellbeing.*'

The ROXANNE consortium is mindful of the potential harmful impacts that could be generated during the development of the platform, and its use. These potential impacts, analysed below, need to be considered holistically and so individual, societal, and environmental wellbeing must be considered together rather than individually, and in conjunction with the other ethical requirements.

[27] See 'Transparency', Cambridge Advanced Learner's Dictionary & Thesaurus, CUP, UK. Available at: https://dictionary.cambridge.org/dictionary/english/transparency
[28] SHERPA Guidelines, p.12
[29] SHERPA Guidelines, p.13

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

Accountability

The SHERPA ethical guidelines supplement the accountability high-level requirement with the sub-requirements of "*auditability, minimisation and reporting of negative impact, internal and external governance frameworks, redress, and human oversight*"[30] explaining the risks related to non-respect:

> "*Because AI and big data systems act like agents in the world, it is important that someone is accountable for the systems' actions. Furthermore, an individual must be able to receive adequate compensation in the case of harm from a system (redress). We must be able to evaluate the system, especially in the situation of a bad outcome (audibility). There must also be processes in place for minimisation and reporting of negative impact, with internal and external governance frameworks (e.g., whistleblowing), and human oversight.*"[31]

In applying these requirements to the ROXANNE project, accountability for actions within the project and in using the potential platform are considered to be of paramount importance. From the below analysis, it becomes evident that there is a need for incorporating user access control and logging mechanisms within the tools design and for properly documenting the system's performance, including any poor results and measures taken to counter those.

Each of these requirements and sub-requirements were used as points of analysis in the Ethics Touchpoint Table, which is a tool developed by TRI in order to provide an overview of the ethical issues in projects such as ROXANNE that will now be discussed.

Ethical analysis

In ensuring that the ROXANNE project follows an ethics-by-design approach, TRI, CAPGEMINI, and INTERPOL have been analysing the potential ethical issues that could be raised by the ROXANNE project activities. The identified issues are being discussed with different concerned parties, such as the technical partners in charge of developing the ROXANNE platform components and the Internal and External Ethics Board members, in order to validate the preliminary findings, and agree on appropriate mitigation steps. The WP3 partners followed a consistent assessment approach in line with the ethical guidelines[32] produced within the SHERPA project[33].

The ethics touchpoint table was developed by TRI who used it to conduct an initial assessment of ethics, data protection, societal, and legal issues. They then discussed concerns raised and potential mitigation strategies with WP leaders to determine if their concerns and mitigations strategies were realistic. This work was then used as a starting point to discuss ethical issues in the project between WP3 partners and to begin a deep analysis of these issues in order to develop benchmark requirements as part of an impact assessment.[34]

It should be noted that as the project progresses and the system is defined, the ethical analysis will become more granular as it will adapt to take into consideration new elements that become available. With the consortium in the initial stages of discussing the project results, exploitation plan, and strategy, the focus and scope of the

[30] SHERPA Guidelines, p.12
[31] SHERPA Guidelines, p.14
[32] SHERPA Guidelines
[33] Shaping the ethical dimensions of smart information systems– a European perspective (SHERPA) project https://www.project-sherpa.eu
[34] WP3 partners split the SHERPA requirements according to their person months for task T3.1 and analysed how the project could comply with them, and how this might impact the project. TRI analysed: human agency, liberty, and dignity; technical robustness and safety; privacy and data governance; individual, societal, and environmental wellbeing. Capgemini analysed transparency. INTERPOL analysed: diversity, non-discrimination, and fairness; accountability.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

ethical assessment will progressively extend from the research and development phase of the project in this document to cover the ROXANNE platform's actual use considerations in later WP3 deliverables. However, some initial considerations about potential use of the platform are incorporated into this deliverable also.

In applying the SHERPA requirements to the ROXANNE project, numerous potential implications have been identified. For a detailed overview of issues arising per project task, please refer to the ROXANNE Ethics Touchpoint Table. In order to sufficiently analyse the development and use of the ROXANNE platform, INTERPOL suggested evaluating the platform across 5 phases of development that are suggested in the SHERPA guidelines: requirement gathering; planning and designing; development; testing; evaluation.[35] These were discussed amongst WP3 partners and it was decided to add 'Phase 6: Use' in order to also consider initial issues that might only be raised following the ROXANNE project. The phases considered are:

- **Phase 1: Requirement Gathering** – In this phase, requirements for how the ROXANNE platform should work are gathered and analysed. These requirements come both from the aims of the ROXANNE project in building the intended platform as outlined in the proposal, and from the requirement surveys conducted in WP2: end-user requirements; end-user training requirements; legal requirements. At this point, ethical concerns are chiefly related to gathering requirements from human participants in an ethical way.
- **Phase 2: Planning and Designing** – In this phase, the partners plan what the platform will do, and how it will work. At this point, ethical concerns are mostly focussed upon ensuring ethical behaviour between the partners. However, planning and designing is also the stage where major decisions about the structure and functionality of the platform are made, that have implications for its eventual legal and ethical use.
- **Phase 3: Development** – In this phase, the partners actually build the platform. At this point, ethical concerns are primarily concentrated on ensuring that partners act in ethical ways when engaging in data processing and developing components.
- **Phase 4: Testing** – In this phase, the platform is tested. At this point, ethical concerns are generally fixated upon how the testing of the platform could impact upon persons whose data is used in testing, and LEA officers who are using a prototype version of the platform during field-tests.
- **Phase 5: Evaluation** – In this phase, the platform is evaluated. At this point, ethical concerns are directed towards ensuring that testing results are listened to and assessed in a fair and equal manner.
- **Phase 6: Use** – This phase is after the project and ethical concerns at this point are focussed upon the impact of the platform on LEA officers, suspects in criminal networks, and innocent people who could, potentially, be caught up in an investigation. Although creating requirements for this phase is beyond the project and the control of partners, recommendations are made for how ROXANNE could be used in a manner that is ethically permissible. It should also be noted that the analysis of the implications for using the ROXANNE platform are limited, as the intended use cases have not yet been developed (T2.3/D2.4, M18), and nor have the precise functions of the system been decided. The next iteration of this report (D3.4, M36) will provide more granular assessment of the implications of the ROXANNE platform in use.

This deliverable now proceeds to evaluate ROXANNE across each of the 6 phases of the project in terms of each of the SHERPA ethical requirements. Each section outlines benchmark recommendations/requirements that, if complied with, should fulfil the ethical requirement, or mitigate an ethical risk. As the project is now in month 14, compliance with some of the benchmarks that are discussed below can be evaluated in the early phases of the project; those for later phases will be evaluated in the next iteration of this deliverable (D3.4, M36).

[35] SHERPA Guidelines, p.21. In the SHERPA guidelines, these phases are used to generally describe an 'Agile' methodology, as oppose to a CRISP-DM product development methodology that is the main focus of the guidelines; the WP3 partners determined that, as they are quite general, these phases would be more applicable to the ROXANNE project.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

Phase 1: Requirement Gathering

A major task of the ROXANNE project is to gather end-user requirements (i.e. technical, operational, legal and training) from the end-user community in order to integrate them into the system design and development of the ROXANNE platform. This will enable the ROXANNE consortium to develop a solution tailored to the experiences and needs of law enforcement. To comply with the diversity, non-discrimination and fairness requirements, it is key to target and collect input from a diverse and representative pool of end-users. To this end, in addition to the 10 partner LEAs, the end-user requirements survey was circulated to the Stakeholder Board members that includes additional LEAs, research and policy-making representatives selected based on their proven expertise and experience. Furthermore, INTERPOL's global network of law enforcement contacts in 194 member countries was leveraged, which further expands the geographical and specialization scope of responders beyond Europe, enabling officers from different background to share their opinion and experiences on the use of voice, text and face technologies. The survey was carried out as part of T2.1, and an analysis of responses is provided in D2.3 (ROXANNE end-user requirements). These responses will also be used to determine how best to develop the decision-making mechanism in T3.6, to ensure that the mechanism takes into account differences in individual countries and can be used across different legal systems.

Owing to the use of human participants in this research activity, issues of human agency, liberty, and dignity are raised by how those who are providing the requirements are treated; these mostly overlap with principles of research ethics, particularly those related to informed consent. In ROXANNE, respondents to the requirement gathering survey are mostly LEA officers and staff. Participants' agency to choose whether to participate was respected, their positive liberty to make choices about their participation was enabled, and their negative liberty to be free to leave their participation at any time was respected by giving respondents full information about their participation and allowing them to make a free choice about whether they wish to participate. These requirements were met as partners provided detailed information sheets with the survey that explained what was being asked of respondents, and, importantly, that they were in control of their participation at all times and could skip questions, or only partially complete the survey if they wished. Further, partners' answers were only evaluated where they consented. Consequently, this benchmark would seem to have been met.

> *Requirement to treat survey respondents with respect for their agency, liberty, and dignity completed .*

This also links with transparency, as it is imperative to provide documentation that provides participants with a clear understanding of how their personal data will be treated. The information sheets that accompanied the survey explained exactly how the personal data of the participants would be treated, and so this requirement can be seen as met.

> *Requirement to be transparent about how personal data will be processes completed.*

In terms of technical robustness and safety, a potential issue during the requirement gathering stage is the safety and security of the systems used. The T2.1 (Collection of end-user requirements) survey gathered responses using both editable PDFs and the EUSurvey platform. Partners were confident that both methods were safe and secure due to having used both methods previously without issue.[36] In addition, partners followed data security measures that were appropriate to the type of personal data being processed (see D10.5, Technical and organisational measures), and processed all personal data in accordance with the GDPR.

> *Requirement to use safe and secure infrastructure to process requirement surveys responses completed.*

In terms of accuracy, reliability, and precision, a potential risk might be that the participants could struggle to understand the survey and what is being asked of them. In order to avoid this issue, each part of the surveys (end-user, end-user training, and legal requirements) were drafted by different partners working together. Then, partners with both technical and ethical/legal expertise reviewed the surveys before they were distributed. Following this, internal LEAs were asked to partake in an initial pilot of the surveys so that any unrecognised

[36] See, for example EU Survey "Privacy Statement", 2020, available at: https://ec.europa.eu/eusurvey/home/privacystatement

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

issues were identified and corrected. Further, the surveys were developed in English and, so that participants who are not fluent in English were able to participate, they were translated into Arabic, Spanish, and French. This was done by the INTERPOL translation service, who provide high-quality translations in order that participants will be aware of what they are being asked to do if they speak one of the other official INTERPOL languages better than English.

Requirement for the requirement surveys to be accurate, reliable, and precise completed.

A key issue for data governance at the point of requirement gathering is how personal data collected during requirement surveys are treated. In order to deal with these issues from an ethical perspective, a primary issue is respect for the privacy of data-subjects. For Solove, data collection can infringe upon a person's privacy where it is gathered through surveillance or interrogation.[37] The ROXANNE partners did not engage in surveillance or interrogation to gather requirements; the data collection was conducted through a survey only.

Requirement for requirement gathering to respect privacy completed.

With respect to data quality, this should ensure that the data is relevant, accurate, complete, and reliable, in order that partners can fulfil the tasks they are planning on using the data for and so that they do not need to return to data-subjects for additional information. The surveys were designed by technical partners who need to gather the requirements in order to produce the ROXANNE platform, these were reviewed by other partners and the consortium is confident that the survey and questions were designed in such a way that data quality can be assured.

Requirement for requirement gathering surveys to ensure relevant, accurate, complete, and reliable data as far as possible completed.

In terms of access to data, responses are being received by NFI who have pseudonymised the responses by removing names and any identifying information in the written answers from the completed surveys. This pseudonymised data will then be accessible to partners who will be analysing the surveys; partners will not try and re-identify participants. As such, the privacy of the respondents will be respected as far as is practicable during the gathering and analysis of requirements.

Requirement to respect the privacy of survey respondents completed.

Further, it is important that people have control over their data in order to ensure ownership and fulfilment of data rights. Owing both to standards of research ethics,[38] and using consent as the legal basis for processing,[39] participants who provide data to ROXANNE partners are given control over their data. This includes allowing participants to determine how much personal data they wish to provide, and if they wish to decline having their data available for future research or included in publications. Participants can withdraw from their participation, or having their personal data processed at any time. Although no data-subject has requested to have their personal data removed, the partners are in a position to do so should such a request be made. It would, therefore, seem that ROXANNE partners are in a position to fulfil this requirement in this phase.

Requirement to fulfil data rights and data ownership of data-subjects on track to be completed.

In terms of diversity, non-discrimination and fairness, the inclusion of survey responders' country of origin, gender or occupational field (i.e. operational, legal or technical) should not have an impact on the weight or importance given to expressed requirements. Partners should treat and analyse all feedback equally. It should be noted that the provision of personal information is optional for responders. Should such information be provided, the analysis will take place on pseudonymised data. During data analysis, partners treated all data equally and fairly. All data was treated as valuable and useful for the project; no responses were discarded because of where respondents came from or who they are.

[37] Solove, D, "A Taxonomy of Privacy", *University of Pennsylvania Law Review*, Vol.154, No.3, January 2006, 477-560 (hereafter: Solove, 2006), pp.491-504.

[38] European Commission, *European Textbook on Research Ethics*, Directorate-General for Research Science, Economy and Society, Brussels, 2010, 35-47.

[39] Art.6(1)(a), GDPR.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

Requirement to not discriminate against participants, and to treat responses fairly, completed.

Individual wellbeing has clear links to respect for human agency, liberty, and dignity mentioned above. When gathering requirements for the ROXANNE platform, treating people with respect for those values would seem to also fulfil requirements of individual wellbeing. With regard to societal wellbeing, gathering requirements has links with diversity and not prioritising particular viewpoints over others. As the requirements survey is being distributed globally across the INTERPOL communications network, and responses will be pseudonymised before being analysed, prioritising particular views would seem to be avoided.

Requirement to respect individual and societal wellbeing during requirement gathering completed.

In terms of environmental wellbeing, avoiding excess use of resources would seem to meet this requirement. Through asking respondents to answer electronically, this avoids a large use of paper if the surveys were distributed in hard-copy, for example. As such, this requirement would seem to have been met by the partners.

Requirement for survey to not use excessive resources completed.

The collection and definition of end-user requirements for inclusion into the ROXANNE system may raise some accountability concerns, as some of the expressed needs may be hard or impossible to reconcile. Therefore, it is important for all the decisions taken pursuant to feedback collection to be appropriately justified and recorded in corresponding deliverables i.e. D2.2 (End-user training requirements), D2.3 (ROXANNE end-user requirements). Similar considerations apply to all the final decisions on chosen requirements to be reflected into the ROXANNE system's setup, user interface, specific tools, etc. As not all decisions following on from the requirement gathering survey have been made, it is not yet possible to determine if this requirement has been met.

Requirement to openly justify decisions based upon the requirement gathering survey not yet possible to evaluate.

Phase 2: Planning and Designing

In this phase, ethical risks are raised in relation to partners being treated with respect and dignity when planning and designing the ROXANNE platform. All partners should: treat each other respectfully; take into account differences of opinion in a fair and balanced way; ensure that no partners or colleagues are forced into situations that they do not wish to be in. There are legal measures available in the Consortium Agreement, but the ethical aim would be to avoid using them. Further, there is an expectation that partners would have their own norms or policies of responsible behaviour and conduct. This benchmark seems to be complied with at this point in the project. Concerns of partners are discussed openly where appropriate and solutions are found; for example, some partners have suggested that there are too many emails within the consortium, and too many meeting were being made mandatory, the project responded to this by using different email lists, and making it clear to partners what is required of them in terms of meeting attendance.

Requirement to treat consortium colleagues respectfully fulfilled up to this point in the project.

To ensure technical robustness and safety, the work of partners in the planning and designing phase is safe, secure, accurate, reliable, and precise, the platforms used for consortium work need to meet these requirements. Partners use Switch Drive for collaborative work. This is regularly used in Swiss academia. It is password-protected and consortium documents are only available to consortium members. It is also encrypted using SSL. It has a system-wide back-up for disaster recovery that is carried out by IDIAP. Thus, it can be said that Switch Drive is safe and secure.

Switch Drive incorporates Only Office that partners use for creating work together. This is very similar to other office software, such as those from Microsoft or Google. Consequently, partners are familiar with this system and can use it without any training. Thus, this would seem to enable partners to conduct their collaborative work so that it is accurate, reliable, and precise; no work will be lost of detrimentally affected because partners are unfamiliar with the system, for example.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

Requirement for planning and designing to be technically robust and safe completed.

During the planning and designing phase, data governance issues primarily relate to respecting the privacy of consortium partners, and of consortium procedures. This should be fulfilled by partners not sharing contact details beyond the consortium without the consent, or reasonable expectation of colleagues, and by not sharing information that the consortium regards as confidential beyond partners. Partners in WP3 are not aware of any instances where such privacy requirements have been violated, and so it would seem to be complied with so far.

Requirement to respect privacy of consortium partners and consortium confidential documents fulfilled so far.

The planning and designing phase is one of the most crucial phases with respect to transparency as an ethical factor. The platform would have to be designed according to the General Data Protection Regulation for the processing of any personal data, whilst also keeping in mind the requirements and provisions of the Law Enforcement Directive for potential uses. Further, the various sources of data collection and data format would have to be accounted for in this phase. All major decisions made in this phase could be discussed with Internal and External Ethics Boards to ensure security, efficacy and ethical compliance of the envisioned platform. This phase could also be used to define the modules/parts of the platform, the information about which would be made public including the extent of this information. This includes selection of training data for the platform. All major decisions about data processing are discussed at bi-weekly calls of the project partners, and any specific queries can be forwarded to the Internal or External Ethics Board, for example; thus, the decision-making about data processing is open and transparent within the project and with stakeholders. Further, the vast majority of technical deliverables that do, or will, discuss data processing are (or, in the case of deliverables yet to be completed, intended to be) public, and so the decisions about data processing will be openly available to the public, thereby providing transparency about the data processing.

Requirement to be open about decisions regarding data-processing in the project completed so far.

In addition to being transparent with the public by making several technical deliverables freely available, it aids transparency to openly demonstrate what the project is doing, and how is it doing it. The project website provides this information, and so this would seem to be completed. A further method of transparency is to display how the public can influence the project, this will be done by collecting feedback from citizens through surveys; this has the added benefit of providing the public with insight into what work is being done and thereby generating trust in the project partners, and the platform in the long run. Citizen surveys on ethical, societal, and legal issues will be distributed soon, following a webinar on these areas.

Requirement to be transparent with the public about the ROXANNE project and its progress expected to be completed.

Algorithmic transparency is another major factor which would have to be considered at this stage. Effectively, technical partners should account for the need to be able to explain the functioning of the algorithms and the outputs by the system. The system should not be a black-box which just generates output based on a complex set of algorithms that are incomprehensible to human understanding. Technical partners should discuss the extent to which transparency can be ensured without hurting the efficacy of the platform, and determine technical measures the ensure that the processing of the ROXANNE platform is be understandable.

Requirement for technical partners to implement measures to ensure data processing by the ROXANNE platform is transparent and understandable to human beings, not yet possible to evaluate.

In considering the potential implications for the requirements of diversity, non-discrimination and fairness during the ROXANNE project planning and designing phase, we should take a closer look at the functioning of the ROXANNE consortium and its decision-making structure. First, the diversity inherent to the project consortium should be noted, it brings together 24 partners representing LEAs, researchers and industry from 16 countries across Europe. As the project unfolds, all issues encountered are open for debate among a mixed and interdisciplinary group, enabling partners from different cultural and professional (i.e. technical, legal, LEA,

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

research, academia) backgrounds to express their views and concerns. The level of individual project engagement is voluntary although proportionate to allocated efforts. Nevertheless, any willing partner is free to engage in deeper, thematic work (i.e. technical, legal, ethical, communication), which contributes to partners' individual control and empowerment of degree of project involvement.

> *Requirement for professional diversity in ROXANNE colleagues completed.*

The design of the ROXANNE system architecture represents another key aspect for fulfilling the diversity, non-discrimination and fairness requirements. This should be achieved by relying on the varied and representative feedback collected in the framework of the previous phase focusing on requirements gathering. As there will be at least three versions of the ROXANNE system throughout the project lifespan, all subsequent system design adaptations should be validated following systematic consultation with a broad and varied range of stakeholders (e.g. Stakeholder Board members, Stakeholder contacts list, field-test participants) in order for the revised system design to represent an improved version that caters for different needs and uses. Partners are committed to the importance of involving a truly diverse and complementary range of stakeholders that would bring varied insights to the project's work by sharing their perspectives. As can be seen in D8.4 (First Field-Test Report and Recommendations), there is a validation process that incorporates feedback from all of these groups and it is expected that the project will follow the same process for the next two field-tests too.

> *Requirement for diverse inputs in validating the ROXANNE platform, completed so far.*

To provide a diverse group from which to receive feedback, all partners are contributing their business contacts to the project stakeholder contacts list constituted of four large groups (policy-makers, LEA, press and other). The consortium's interdisciplinary (industry, LEA, SME, academia and research institutes) nature further strengthens the efforts in this regard, as does its geographical diversity (24 partners from 16 countries). INTERPOL also leverages its global membership to disseminate the project among the international LEA community and to identify interested stakeholders for project involvement.

> *Requirement to have a diverse group from which to gather feedback from completed.*

Diversity within project partners would also likely add to the overall diversity of inputs to the ROXANNE platform. The policies and make-up of project partners is beyond control of the consortium. However, we can recommend that project partners consider developing diversity policies for their organisations if they do not have them.

> *Recommendation that project partners develop diversity policies if they do not have them, not yet evaluated.*

During this phase, individual and societal wellbeing requirements would seem to be met by complying with the human agency, liberty, and dignity, and diversity requirements respectively. With respect to environmental wellbeing, this requirement would again seem to be met by avoiding excessive consumption of resources. For example, partners flying, or otherwise travelling, across Europe for frequent meetings that could be completed using teleconference software would not seem to meet the requirement. So far during the ROXANNE project, partners have had the kick-off meeting, and a technical meeting with an external LEA as face-to-face meetings, owing to the ongoing Coronavirus pandemic. However, most meetings were planned to happen via teleconference software before the pandemic-induced lockdowns occurred across Europe. Therefore, partners would seem to be meeting this requirement so far. In any case, during lockdown all meetings occurred via teleconference software and there are no indications that the frequency of physical meetings will be excessive in future.

> *Requirement to respect individual and societal wellbeing during planning and designing, completed.*

> *Requirement to not travel excessively for face-to-face meetings, completed so far.*

The entire project management, including planning and design in relation to the ROXANNE platform entails potential accountability risks due to possible power imbalances within the consortium. However, the partners adopted a democratic approach of consortium-wide deliberations of project issues, risks and output quality issues in the context of bi-weekly project meetings and thematic meetings (i.e. technical, legal, dissemination).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

All decisions and discussion points are documented in meeting minutes, which are available to all partners for consultation and amendment if necessary. These collaborative fora enable the adoption of decisions pursuant to a predominantly consensus-based approach. All partners have full visibility over pending work and reports in centralised files stored on the Switch Drive, that also lists all upcoming deliverables, partners in charge of them, contributors as well as peer-reviewers. Additionally, the peer-review of all deliverables is coordinated in advance, involving at least two partners, one technical and one outside the WP in question and assigned randomly. The identified risks, completed progress, and work quality are documented in regular reports submitted to the EC (i.e. D1.2 Risk Assessment, D1.4 Internal progress and quality planning report Y1, D1.5 Internal progress and quality planning Y2, D1.6 Final progress report).

Requirement to implement accountability structures completed.

Requirement to hold partners to account for the quality of their work completed so far.

Phase 3: Development

During development of the ROXANNE platform, respect for human agency, liberty, and dignity would seem to be most relevant to the persons whose data is being processed in order to develop the platform. This relates both to initial data collection by the project, and re-using datasets from previous research activities.

In terms of data collection, this should involve treating research participants according to research ethics standards.[40] The use of human participants in collecting voice data in T4.6 Target data simulation for development and demonstration activities and T5.2 Speaker identification, diarization and role recognition in multiparty interaction, and during interviews/workshops in WP8 should enable participants to exercise their agency and liberty to leave the research activity at any time, and be treated in a dignified way. These tasks are in progress. Nevertheless, it is made clear to participants on the information sheets and informed consent forms that they are free to leave research activities at any time, without negative consequences, and so this ethical benchmark is being complied with and we expect this to continue. In terms of dignified treatment, participants have, so far, be recruited in a transparent and fair manner, and are being treated with respect; we expect this to continue.

Requirement to treat human participants involved in data collection respectfully completed so far.

With regard to re-using datasets, this involves respecting the persons whose data is contained in datasets to be reused and only using datasets that were created using proper safeguards. The use of datasets created by universities and research institutes should meet this requirement as it most likely that the data was gathered or collated into a dataset with oversight by a research ethics committee and, at the very least, according to a framework of research ethics. All datasets currently planned for repurposing were created by university researchers, and so this ethical benchmark has been met at this stage. The ethical governance of research datasets should be considered by technical partners before deciding to use them. The project will likely use more datasets as the project progresses and the ethical implications of these will be considered when they are selected.

Requirement to only re-purpose datasets that were created subject to a research ethics framework fulfilled up to this point in the project.

Requirement for technical partners to check that data to be re-purposed was gathered ethically, to be completed.

Another aspect of re-using datasets is only using them in the ways that data-subjects would expect. For example, attempting to re-identify data-subjects would not be within the expectation of persons who provided their data for these datasets. In general, the ROXANNE partners are using these datasets for research and so this

[40] See, for example, European Commission, *European Textbook on Research Ethics*, Directorate-General for Research Science, Economy and Society, Brussels, 2010.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

does meet the general requirement. More specifically, ROXANNE partners are using these datasets to build computer models for recognising entities in speech, text, video, and for network analysis. Thus, they are being used to contribute to building something of scientific benefit, which would come within the likely expectation of persons providing data for research. Additionally, there will be no direct effects for data-subjects; no decisions will be made about them using their data. There is a risk that persons whose data are used in the speech/text/video recognition models might be slightly better recognised by the ROXANNE platform in future than if their data was not used, but this has been assessed by the partners to be very low – in any case, the ROXANNE consortium only intends for the platform to be used by responsible LEAs and so it can be anticipated that any person who is highlighted by the platform at a higher incidence than persons whose data was not used for developing the models would be treated lawfully. Overall, the re-use of data in the development phase would not seem to be in contravention of the agency, liberty, or dignity of persons whose data is used.

Requirement to use data in ways that data-subjects would expect completed so far.

Requirement not to create problematic effects for data-subjects completed so far.

The development phase is clearly the prime opportunity to build the ROXANNE platform so that it is the best that it can be. If we look forward to the use phase, we can see the importance of this. As ROXANNE will analyse data from pre-existing LEA systems, this means that the raw data might come from systems that are old or have a lot of 'noise' in them, for example older, low-definition CCTV cameras. The analysis of noisy data can result in higher levels of false positives and false negatives than in data with less noise; this is particularly relevant to the use of ROXANNE if lawfully obtained data in an investigation comes from systems that include lots of 'noise', for example, use of facial recognition tools by ROXANNE could be affected by the quality of data coming from CCTV cameras that are old and do not provide high-definition images.[41]

Further, if ROXANNE is used for analysis of several data types simultaneously, and there is lots of noise in the data, then this could result in the false negatives/positives being compounded and the overall output of the combined analysis producing a larger probability of error.[42] The effect of this is that substantial numbers of people could be wrongly highlighted or missed by the ROXANNE platform. The primary implication of this is that innocent people could be subject to an unnecessary intrusive investigation by LEAs, and people whose activities should be investigated are not considered by LEAs. Thus, this provides a clear impetus to technical partners in ROXANNE to ensure that the platform is as accurate, reliable, and precise as possible when classifying people and their behaviours.

Requirement for platform development to be accurate, reliable, and precise not yet possible to evaluate.

With regard to safety and security, ethical risks include the loss or unauthorised access to the underlying code for what is a high-risk technology. Development of code for the ROXANNE consortium will take place using the GIT platform. ROXANNE partner LUH provides the installation of GIT on their own servers. LUH provides access to GIT only for manually whitelisted accounts from the ROXANNE project. Only these accounts can access data on the GIT. GIT is encrypted using SAML SSO and enforced two-factor authentication. Additionally, data is backed-up to LUH servers. Consequently, development of the underlying ROXANNE code would seem safe as it is protected from loss, and is secure as it is protected from unauthorised access.

Requirement for code development to be safe and secure completed.

During the development of the ROXANNE platform, privacy is an issue in relation to use of pseudonymised data, and to secondary use of data. With regard to pseudonymised data, if partners were to re-identify data-subjects (either participants who have provided their data to the consortium, or persons whose data is contained

[41] Hern, Alex, "What is facial recognition – and how do police use it?" the Guardian, 24 January 2020. Available at: https://www.theguardian.com/technology/2020/jan/24/what-is-facial-recognition-and-how-do-police-use-it

[42] See, for example, Whitehorn, Mark. "Decision time for AI: Sometimes accuracy is not your friend" The Register, 6 July 2018. Available at: https://www.theregister.co.uk/2018/07/06/accuracy_in_machine_learning/

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

in datasets from other research projects), then this would violate the privacy of such persons. Pseudonymisation and anonymisation protect people from biases against them, from reprisals for their views, and from data processors being able to connect information in order to reveal insights into a person.[43] Consequently, re-identification of pseudonymized or supposedly-anonymised data-subjects would put them at risk of such harms. Thus, not identifying persons would seem to meet this sub-requirement. ROXANNE partners have no intention to re-identify such persons and so are on-course to meet this requirement. Its fulfilment, however, can only be judged once the processing of these data is completed.

> *Requirement not to re-identify data-subjects in pseudonymised or supposedly-anonymised data, completed so far.*

Re-purposing of data also creates ethical issues in relation to privacy.[44] First is whether persons consented to their data being used for purposes additional to, or other than, the original processing. Where people consensually provide data for a research project in the knowledge that their data will be used for other research projects of a similar nature, this would seem to not violate their privacy.

However, if a person does not consent to their data being re-purposed, or it is used in a way they do not expect this would violate their privacy.[45] Even if this is the case, re-purposing of data can be benign.[46] The research carried out using re-purposed data in the ROXANNE project has been benign so far. All data to be repurposed already comes from datasets that have been created specifically for research purposes, and: the data-subjects consent to this, or; the original data was made manifestly public by the data-subjects, or; is a matter of public record.

Where data-subjects consented, this re-purposing would not seem to be a violation of their privacy. Data that was made manifestly public comes from television shows and interviews, and data that is a matter of public record are reports of criminal activities that were reported in the news. As the data-subjects did not specifically consent to their data being used for research purposes, this is a minor infringement upon their privacy. However, as these data are already in the public sphere, re-purposing of them does not to create an additional infringement on privacy. Consequently, processing of such data would not seem to violate the privacy of such data-subjects to a degree that would prevent these datasets being used. The overall fulfilment of this requirement can only be assessed once the project has finished processing data to test and validate the computer models. Other datasets which the project decides to use in future will be assessed on this same basis; there is currently no plan to use LEA data from real (closed) cases in the development phase.

> *Requirement to respect the privacy of data-subjects when re-purposing data generally fulfilled so far. Fulfilled where data-subjects consented to re-purposing, minor and benign infringement on privacy where data is gathered from the public sphere.*

In terms of transparency in this phase, emphasis should be on the dissemination of results and progress made by the project. Any data which is deemed non-confidential but shows such progress, can be used for this purpose. For instance, the results from the planned field-test could be used shared. This would keep all relevant stakeholders and the public well informed about the project and promote awareness about the purpose of this platform. Further, the consortium should be open with organisations that serve a regulatory function, such as national data protection authorities, if they request information. In addition, project partners should also be open with oversight bodies, such as the EC and Ethics Boards if they request to discuss certain parts of the project. In order to facilitate this openness, partners should maintain accurate records of their activities, especially their processing of personal data.[47] Part of this recording can be seen in the Ethics Deliverables that the consortium has provided to the EC (WP10), and discussed with the Ethics Boards. Whilst these documents are confidential to the partners and the EC, partners should be as open as possible about the information in them (and about their processing operations) with regulatory or oversight bodies.

[43] Solove, 2006, pp.513-515.

[44] Solove, 2006, pp.518-520.

[45] Solove, 2006, p.520.

[46] Solove, 2006, p.519.

[47] Art.30, GDPR

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

> *Requirement to disseminate non-confidential results, to be completed.*
>
> *Requirement to be open with regulatory and oversight bodies, not yet possible to evaluate.*
>
> *Requirement to maintain accurate records of data-processing and ethical decision-making, to be completed.*

Another important aspect, with respect to a technically intricate platform such as ROXANNE, is that of algorithmic transparency. It refers to

> *"One, or more of the following aspects: code, logic, model, goals (e.g. optimisation targets), decision variables, or some other aspect that is considered to provide insight into the way the algorithm performs. Algorithmic system transparency can be global, seeking insight into the system behaviour for any kind of input, or local, seeking to explain a specific input - output relationship."*[48]

Algorithmic transparency will help researchers understand how exactly the complex platform is working and how it can be further fine-tuned to increase efficacy and decrease any possible flaws. For regulators, it is a way to understand if the platform is being used in a legal and ethical way. Further, it helps the public understand how the platform works, and how the data is being used to reach an outcome or insight. Algorithmic transparency often helps the public in challenging the technical platform/system in question, and hence instils a sense of security. As for the LEAs, it will be useful to understand the platform so that they know how it works, what may go wrong and how to use it effectively. In essence, this sense of security/trust may be attributed to better awareness and knowledge about the platform which in turn reduces the fear of unknown. In contrast, complete algorithmic transparency might make it easier to find loopholes in the system, which might risk the efficacy of the entire platform. Further, the requirement for transparency might even lead to use of sub-optimal algorithms, which again could seriously harm the purpose of such a platform.[49]

> *Requirement to provide the public with an understanding of how the ROXANNE tools work, to be evaluated.*

There is a need to strike a good balance to ensure optimal algorithmic transparency. The LEAs or end-users must be compliant with respect to transparency requirements, to ensure that any decision or outcome can be audited or challenged by the regulators or supervising body. The public should be privy to at least basic functioning of the algorithms and the flow of data so as to have an opinion about the trade-offs, benefits and risks associated with such algorithms. Hence, the platform should be designed in a manner that the LEAs can support the outcome of the system and defend the same using the documentation related to algorithmic transparency and functioning of the system.

> *Requirement for technical partners to build the platform to enable LEAs to be transparent by making the algorithmic decision-making explainable so that results can be audited and challenged by supervisory authorities, not yet possible to evaluate.*

With regard to non-discrimination, a fundamental concern in data-driven analytical tools such as the ROXANNE platform is the potential reliance on biased datasets to build, improve and/or test the technologies under development as this would results in a skewed product. Whatever the motivations of end-users, use of biased data can create biased tools which have biased effects during use.[50] This would not only be counterproductive for LEA purposes but poses serious ethical, societal, and legal concerns. As part of the initial development of speech, natural language processing, and video technologies, partners must ensure their data model is built on unbiased, gender-balanced datasets to avoid unfairly targeting certain population groups who are disproportionately captured in policing data. In their survey of potential data resources for building and

[48] European Parliament, "A governance framework for algorithmic accountability and transparency", EU, 2019. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624262/EPRS_STU(2019)624262_EN.pdf

[49] European Parliament, "A governance framework for algorithmic accountability and transparency", EU, 2019. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624262/EPRS_STU(2019)624262_EN.pdf

[50] See, for example, Benjamin, Ruha, *Race After Technology*, Polity Press, Cambridge 2019, p.165; Valentine, Sarah, "Impoverished Algorithms: Misguided Governments, Flawed Technologies, and Social Control" *Fordham Urban Law Journal*, Vol.46, No.2, pp.364-427, pp.370-371

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

training purposes of the ROXANNE platform, partners need to ensure that they identify and rely upon a diverse enough sample of resources to avoid training the technology on non-representative datasets which will result in prejudiced and unfair outcomes for the developed technology.[51] To this end, the selected data needs to account for the diversities of potential individuals of interest, taking into consideration aspects such as language, accent, socio-economic background, age, and gender groups. Similar considerations persist during the subsequent testing aimed to enhance the underlying technological components of speaker identification systems, diarization and role recognition. Therefore, it is important to counter from the outset any potential discriminatory influences that may prejudice the outputs by including a diverse range of (speaker) profiles and models, while avoiding unjustified focus on certain groups or categories.

> *Requirement for ROXANNE to be developed using datasets that represent diverse populations in terms of language, accent, socio-economic background, age, and gender, not yet possible to evaluate.*

Individual wellbeing could be affected during the development phase if colleagues are put under significant pressure to complete the platform in a short time-frame. Whilst working toward a deadline often involve intensive work, this can affect individual wellbeing if the expectation for output is excessive and colleagues are pressured into working overtime. Thus, in order to meet this requirement, partners should plan development so that work is not excessively loaded towards the deadline. So far, partners are meeting this requirement

> *Requirement for partners not to put colleagues under excessive work pressures completed so far.*

With regard to societal wellbeing, drawing upon the user-requirements should enable the ROXANNE platform to be developed in such a way as to fulfil the needs of stakeholders and wider society as far as they are representative of it. However, as the actual development of the platform has a limited interaction with wider society, it is difficult for this phase to have direct impacts on societal wellbeing and so it is also difficult to determine specific requirements for partners to meet. Having said that, the work on societal values (T3.2, Comply with societal values, below) continues to gather views of citizens on societal issues. Consequently, while citizens cannot directly engage in the development of ROXANNE, they can have influence by providing feedback in relation to societal values. Consequently, by implementing this feedback, the ROXANNE project can ensure that the platform is compliant with the societal values discussed.

> *Requirement for development of the ROXANNE platform to be compliant with societal values, not yet possible to evaluate.*

In terms of environmental wellbeing, data processing platforms are already highly-energy intensive and so building a system that carries out more data processing than other technologies clearly raises environmental issues.[52] As ROXANNE is intended to process multiple data-sources, it could, depending upon the way in which the platform is developed, be more or less energy efficient that having separate systems for each data source. As such, partners should endeavour to produce a platform that has a lower energy usage than separate systems, but also having regard to the fact that this might not be possible as each data analysis component is novel and so cannot be directly compared to a pre-existing system. This could include, for example, having technical partners consider energy efficiency as a metric to be considered when they make decisions about how the ROXANNE platform should be developed.[53] As the development of the platform is still ongoing, it is not yet possible to evaluate this.

> *Requirement for technical partners to give regard to energy efficiency when developing the platform and to endeavour to build a platform that does not consume disproportionate amounts of energy, not yet possible to evaluate.*

[51] See, for example, D'Ignazio, Catherine, and Lauren F. Klein, *Data Feminism*, MIT Press, Cambridge, Massachusetts, 2020, p.123.

[52] On the environmental impacts of data use, see Jones, Nicola, "How to stop data centres from gobbling up the world's electricity" Nature, 2018. Available at: https://www.nature.com/articles/d41586-018-06610-y

[53] See Pereira, Rui, et al. "Energy Efficiency across Programming Languages" Proceedings of the 10th ACM SIGPLAN International Conference on Software Language Engineering, October 2017, pp.256–267. Available at: https://doi.org/10.1145/3136014.3136031

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

With regard to accountability, technical partners' decisions on which research results and user requirements should be integrated into the development of the ROXANNE technologies, i.e. speech, video technologies, network analysis, should be justified and documented. For example, when processing data for the development of the ROXANNE platform, the technical partners will agree upon the common data interchange format to be applied to data coming from different sources. The adopted decisions should be reflected in corresponding deliverable, following internal debate and consideration of associated advantages and concerns. Although these documents are not open to the public by default, either due to IPR considerations, or requiring access rights for Switch/GitLab or depending on their level of classification (i.e. restricted, classified, public), their existence enables competent and authorised persons outside the consortium to audit the system design should such need arise. In addition, the ROXANNE platform and its technological components must reflect the legal and ethical requirements identified within WP3 and WP10 in line with the pursued privacy and ethics by design approach. To this end, TRI, CAPGEMINI, and INTERPOL will consider with the technical partners how best to integrate into the tools' design legal and ethical safeguards without undermining the tools' functionality while responding to end-users needs and requirements. In addition to legal accountability measures that exist for each partner under their national law, the project entails three levels of accountability to ensure the system's adherence to good ethical practices:

- First, the Internal Ethics Board discusses its analysis findings with the rest of the consortium, before the External Ethics Board scrutinizes these in ethics deliverables (WP10) or specific discussions.
- Second, the EC itself presents an additional level of oversight of the project's ethical dimension through its ethics checks and continuous monitoring of project deliverables, especially within WP3 and WP10.
- Finally, the project is also subject to public scrutiny hence the need to communicate to the civil society on the project's work and its ethical dimension and consideration.

Requirement to integrate legal and ethical considerations into the development of the ROXANNE platform, not yet possible to evaluate.

Requirement for project partners to be subject to legal and ethical accountability measures completed.

Integrating specific technical means within the ROXANNE system's design is essential for complying with accountability requirements on the platform's use. The ROXANNE system architecture foresees user management and access control, including central authorization and authentication services as well as logging mechanism. The elaboration of the ROXANNE case management system should provide due consideration to accountability concerns by defining individuals' access rights and eligible purposes for consulting data. Taking a closer look at specific instances, for example, the platform secure data export and exchange functionality will keep logs on users, information shared, purpose and recipient. If technically feasible, when developing vision-based algorithms to support video location and face verification, records of particular pattern or location for video indexing and linkage purposes could help mitigate possible abuse of the tool. In addition, the platform's relation extraction function could keep records of auxiliary information that served as basis for the extraction. The ROXANNE system data visualisation and exploratory analysis technique should enable human oversight as opposed to a fully automatic and deterministic result. Such technical means (i.e. confidentiality regime, adoption of encryption, choice of standard) to protect information in line with the legal requirements have not yet been developed, but once they are they should be reported to the project supervisory bodies (Ethics and Security Boards) as well as to the EC.

Requirement for technical partners to develop the ROXANNE platform with technical means (e.g. logging mechanisms) to evidence compliance with accountability measures, not yet possible to evaluate.

Phase 4: Testing

In the testing phase, issues of human agency, liberty, and dignity relate to the use of human participants who engage in testing of the platform. As mentioned earlier, human participants have their liberties enabled by them

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

having a free and informed choice whether to participate and have their agency fulfilled where they are able to withdraw from participation. Participants would seem to be treated in a dignified manner where researchers treat them with respect. The testing phase of the ROXANNE project is not yet occurring, but current plans outline that these practices will take place and the agency, liberty, and dignity of participants will be fulfilled/respected.

Requirement to treat participants testing the ROXANNE platform with respect not yet possible to evaluate.

It is unlikely that any platform can function perfectly, we have already noted the risks of false negatives and false positives, and in, conjunction with human dignity, there would seem to be an ethical obligation to communicate to users in a meaningful manner the level of accuracy achievable in the platforms outputs, across different contexts of use. This is particularly pertinent in the ROXANNE project, owing to the nature of the platform and the potential negative effects that could be caused for individuals and society if the platform is inaccurate, unreliable, or imprecise. It would be responsible for the project to devote some effort in trials to understand these levels of accuracy and inaccuracy. This is important so that such issues can be dealt with during evaluation and improved before the platform is used in actual investigations.

Requirement to assess the accuracy, reliability, and precision of the ROXANNE platform not yet possible to evaluate.

It is currently unclear what data will be used in the testing phase, particularly in the case of whether LEA data will be available. If parts of research datasets that were not used in the development of the system (i.e. separated out into a 'test' dataset), then the ethical issues in relation to data governance and protection would be the same as those mentioned in the previous phase.

However, if LEA data is used, then this can generate other issues. If this data comes from real cases, then this poses an ethical issues about how the results will be used and how they can affect investigations. Consequently, the ROXANNE partner decided that they will not seek to test the platform on real ongoing cases, as originally envisaged.

Requirement not to use the ROXANNE platform on ongoing LEA cases completed.

Instead, ROXANNE partners have opted to seek testing of the platform on data from real closed cases that have been thoroughly investigated, with all leads considered closed, and the case is regarded as completed by an authority such as a prosecutor or court in the partner country. Only LTEC has expressed an intention to process real data from closed cases, for which they have permission from the relevant Lithuanian prosecutor (see D10.10, Personal data relating to criminal convictions/offences; also note that the testing has not yet occurred).

Requirement to only process closed cases with appropriate approval, completed so far.

Still, with regard to privacy, data-subjects would likely not have consented to their data being initially processed in an LEA investigation. Of course, society generally accepts this where necessary, proportionate, and lawful in criminal investigations. Consequently, LEA partners should only consider data that was lawfully gathered. We assume that any LEA data from real closed cases made available for use in the project was gathered legally, and, therefore, the original violation of privacy to gather the data was justified. LTEC have confirmed that the data they intend to use in the project was gathered in accordance with Lithuanian law.

Requirement for LEAs to ensure that any data from real closed cases made available to the project was lawfully gathered, completed so far.

However, use of such data in a research project might not come within the expectation of the data-subject, nor society. This is particularly the case where data about innocent people is captured as part of an LEA surveillance operation and their data is contained in a dataset. It would seem to be a violation of privacy for the data-subjects in an ethical sense to use this data, particularly that from innocent individuals whose data is contained in the dataset through no fault of their own, and, potentially, no knowledge of it.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

LEAs should, therefore, consider whether it is proportionate to include data-subjects in the datasets they use for testing. LTEC have considered this and believe that the benefits of helping to develop the ROXANNE platform outweigh possible harms to data-subjects, for which they have implemented technical and organisational measures to reduce.

> *Requirement for LEAs to assess the privacy implications for data-subjects included in their testing data-sets, completed so far.*

Use of such data in the project, even in a pseudonymised or anonymised form, could be seen as an additional violation of privacy as the individuals concerned would not be in a position to consent. As with re-purposing data for development, the question becomes whether this is benign, and can be justified.

The testing of the ROXANNE platform by LEAs is intended to involve evaluations on the efficacy of the ROXANNE tools for use in criminal investigations, and should not be used to make decisions about, or create effects for, data-subjects. During testing, all LEAs will be informed that ROXANNE tools are prototypes and not finished, and so should not be used for making any decisions regarding operations. Consequently, there should be no additional effects for the data-subjects. In this case, processing of personal data from real closed cases would seem to be a minor and benign infringement on their privacy.

> *Requirement for any LEA use of data from real closed cases to be restricted to benign infringements on privacy, expected to be completed.*

Owing to the sensitivities of data from real closed cases, LEAs, and the consortium, need to strongly justify why they need to use such data rather than other data (e.g. synthetic). LTEC have stated that use of synthetic data presents a risk of misjudging the capabilities and accuracy of the ROXANNE platform, and so there is a need to use data from real closed cases in order to properly evaluate the platform.

> *Requirement to justify any use of LEA use of data from real closed cases, completed so far.*

By the nature of subjecting data to new analytical methods, new knowledge can be generated. In the case of using data from real closed cases, this poses a risk of incidental findings through finding previously undiscovered information about a closed case. If information relevant to an illegal activity is found, then partners should follow the incidental findings policy of the project and report it to an LEA who can investigate the new information. This would be a further breach of privacy, but, as this will be to verify whether a crime has occurred, it would seem justified. As testing has not yet taken place, no situations involving incidental findings have occurred.

> *Requirement for any discoveries of illegal activity during data-processing to be reported in accordance with the incidental findings policy, not yet possible to evaluate.*

Use of LEA data also raises issues of data quality due to some LEAs having histories of discriminatory policing practice, such as higher incidences of policing members of ethnic minority groups, and the effects of this being seen in LEA data. Consequently, LEAs should ensure that the data they are using is unbiased as far as is practicable. This is important as positive test results that show the platform working well on biased data would simply add to the reinforcement of biases. The dataset intended to be used by LTEC is very small and so it is not practical to assess the diversity of this dataset.

> *Requirement for LEAs to assess the diversity of their testing datasets where practicable, completed so far.*

Fulfilment of data rights raise particular issues for the use of LEA data. Such data will most likely have been gathered under the Law Enforcement Directive (LED), or precursor legislation. As such, it is difficult for data-subjects to exercise their rights as the LED only provides a right of access for data-subjects, and only where this is not limited by member state law. Consequently, it would be advantageous in ethical terms for the use of LEA data to come under the GDPR. LTEC have stated that they will be testing the ROXANNE platform under the

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

GDPR. Conversations about data availability for other LEAs are ongoing but it is expected that this testing will be regulated under the GDPR. As these conversations are ongoing, it is possible that data-processing during testing could take place under the LED, if this happens then it will be in strictly limited circumstances.

> *Requirement for use of LEA data in the ROXANNE project to be regulated under the GDPR, or under strictly limited circumstances if the LED is applicable, completed so far.*

In terms of access to data and data ownership, however, the sensitive nature of LEA data means that it would be preferable from an ethical point of view for LEA data to remain with LEAs. At this stage of the ROXANNE project, there is no plan that technical partners will be provided with LEA data. However, a ongoing discussion about the possibility of sharing some anonymous or statistical data is ongoing.

> *Requirement for LEA data from real closed cases to remain with LEAs, completed so far.*

In terms of transparency, the testing phase is similar to the development phase in primarily requiring active dissemination of technical progress made in this project. In particular, the public can be informed about how the platform is tested and what the efficacy of such a platform is in terms of the project objectives. This could include test results reflecting lack of bias or sensitivity to any particular attribute of a data-subject as envisioned in the design phase. The efforts should be directed towards being open about possible drawbacks or unintended/unexpected results after testing. The first-field test has taken place, and efforts to disseminate the results are ongoing .

> *Requirement for partners to publicly disseminate results of field-tests, set to be completed.*

Another key aspect of transparency in data-driven technologies, is, as discussed above, algorithmic transparency. In the testing phase, this is important in order to enable persons testing the platform to see how the platform works and make suggestions about how it can be improved, it is also key for technical partners so that they can understand how to make improvements to the platform.

> *Requirement for technical partners to build the platform in such a way to be understandable to persons testing the platform.*

The ROXANNE project relies on continuous testing and the organization of three field-tests to improve the ROXANNE system by identifying and addressing shortcomings in the constituent technologies. The three field-tests, one foreseen each year of the project, present an opportunity to demonstrate to a large audience the level of maturity and efficiency of the ROXANNE system. These demonstrations could potentially entail a discriminatory risk should the platform be tested on a biased algorithm, resulting from selection and reliance on an insufficiently varied and representative range of datasets. However, this risk should be minimised by adequately addressing these aspects in the preceding phases focusing on data understanding, preparation and modelling (WP 4, 5, 6, 7). Similar to field-tests, the continuous testing may pose a risk of discriminatory effect should the chosen datasets not be varied and representative enough. Further to the preventive measures taken in the framework of WP4, 5, 6 and 7 to counter data bias, this risk should be also mitigated by the diversity of partner LEAs that will test the system individually, representing different cultures, languages and specialising in different crime areas.

> *Requirement for technical partners to evaluate algorithm for bias and take steps to reduce this, not yet possible to evaluate.*

> *Requirement for test datasets to be varied and representative, not yet possible to evaluate.*

Individual wellbeing is clearly relevant during testing as this is the point where participants will partake in using the platform and providing their views on it in interviews/workshops. However, the issues related to how such persons are treated by researchers are covered in relation to human agency, liberty, and dignity. Yet, how the participants interact with the platform is also relevant to the individual wellbeing of participants.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

During testing and use, there is an ethical risk of anthropomorphising the ROXANNE platform. When people are confronted with leaps of technological advancement, it is not unusual for them to view a technology as having human qualities. For example, DeepMind's AlphaZero system that plays the board game Go has been described with human qualities of '*insight*' and having a '*breed of intellect*'.[54] This system is of course, simply a machine. Anthropomorphising machines can create an emotional connection between the user and machine; for example, the destruction of military robots from enemy actions can cause a quasi-grief for its users.[55] This could be a particular issue with ROXANNE, as it already has a human name. The effect of anthropomorphising the platform is that it might be seen as more than a mere tool, and can be seen as 'special' to the point where its outputs are treated more favourably than if it were not anthropomorphised.[56] If the outputs of the ROXANNE platform are viewed as special, then this could lead LEA officers down an erroneous path possibly resulting in innocent individuals being arrested or taking longer to find the actual offenders.

A potential solution to this would be including information in the training provision to the effect that whatever the name and potential for human-like qualities to be observed in the ROXANNE platform, it is merely a data-processing system and any human-ness that might be perceived to be present in the platform is an illusion.[57] Further, any exploitation activities should not attempt to further anthropomorphise the tool, and partners should consider renaming the platform prior to actual exploitation. These requirements can only be evaluated later in the project if the suggested actions take place at the appropriate time.

> *Requirement for training provision to make clear that the ROXANNE platform is a machine and should not be anthropomorphised, not yet possible to evaluate.*
>
> *Requirement for exploitation of the platform to not anthropomorphise it, not yet possible to evaluate.*
>
> *Recommendation for exploitation partners to consider changing the name of the platform to a non-human name, not yet possible to evaluate.*

In terms of societal wellbeing, it is difficult to view impacts on society at large during testing as the actual tests of the platform will take place in a separate environment away from actual LEA operations. Thus, the effects of the test cannot create material impacts on society.

With respect to environmental wellbeing, the ecological impact of carrying out field-tests will in large-part come from the travel from across Europe (and beyond) to attend the tests (if physical tests are possible during the ongoing pandemic). As with the development phase, this requirement would seem to be met where travel and meetings are not excessive. The project has planned to hold three field-tests across the life of the project. In light of the proposed ROXANNE platform involving development of many novel components, three field-tests would not seem excessive. However, partners should consider which personnel they are sending to attend field-tests, and whether this is necessary. This will be evaluated following physical field-tests.

> *Requirement for partners to only send necessary persons to field-tests and meetings, not yet possible to evaluate.*

The choice of data to be used for testing and demonstration purposes in the context of the three project field tests will have to be carefully made taking into consideration previously identified risks, such as data bias. With regard to accountability, the discussions and decisions that lead to the final choice need to be deliberated among the consortium and where possible with the involvement of a wider stakeholder group (i.e. Stakeholder Board, Ethics Boards). Conversations about possible LEA data that could be used in the project are ongoing. The rationale behind these decisions will be included in relevant deliverables for accountability purposes. In particular, should some partners access real LEA data to test the ROXANNE platform, this should specify who

[54] Strogatz, Steven, "One Giant Step for a Chess-Playing Machine", *The New York Times*, 26 Dec 2018. Available at: https://www.nytimes.com/2018/12/26/science/chess-artificial-intelligence.html

[55] See, Singer, P.W., *Wired for War*, Penguin, USA, 2010, pp.337-340

[56] Waytz, Adam, Joy Heafner, and Nicholas Epley, "The mind in the machine: Anthropomorphism increases trust in an autonomous vehicle" *Journal of Experimental Social Psychology*, Vol. 52, May 2014, pp.113-117.

[57] See Principle 4, EPSRC, "Principles of Robotics" 2018. Available at: https://epsrc.ukri.org/research/ourportfolio/themes/engineering/activities/principlesofrobotics/

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

accessed, what type of data and under which circumstances (i.e. on premise, remote access) and for the testing of which particular technology component. Similarly, partners in charge of developing simulated data for testing the ROXANNE system, including the definition of scenarios with the help of the internal LEAs, should update the rest of the consortium on the status of their work, the rationale for choosing specific channels/scenarios/languages as opposed to others. This will ensure collective validation of decisions following assessment of associated risk and benefits. Furthermore, the corresponding deliverables will document the arguments and reasoning behind the decisions made by the consortium. These topics will be evaluated when testing take place and any access to LEA data by technical partners happens, if this occurs.

> *Requirement for test data choices to be discussed amongst the consortium and potentially wider stakeholder group, not yet possible to evaluate.*

> *Requirement for any technical partners accessing LEA data to log the circumstances of this, not yet possible to evaluate.*

Phase 5: Evaluation

The evaluation phase is focussed on acquiring and understanding feedback from field-test participants. Human agency and liberty is enabled where participants/partners are able to contribute to a feedback process. Dignity is respected where all responses to the feedback process are treated fairly and equally. This phase of the ROXANNE project is not yet occurring, but we can expect that feedback on testing from individual LEA officers will follow a similar plan to that for gathering feedback from the field-tests and so compliance with these requirements to be fulfilled.

> *Requirements for participants to be able to give feedback and for responses to be treated fairly and equally not yet possible to evaluate.*

A fundamental issue in the development of computer models is that they will include assumptions made about the data and how the model should use these data. This will affect the accuracy, reliability, and precisions of the models. Whatever the choices and assumptions made when creating the models, these will affect the outputs of the algorithms.[58] To some degree, this is inevitable; people will always make different assessments. There is a particular risk in relation to technical partners creating models for use by LEAs as technical partners might bring inaccurate assumptions to their work.

An obvious solution to this would be to follow the requirements gathered in Phase 1. This should certainly happen as much as possible. However, owing to the complexity of the models and the fact that the needs of the models will develop as the project progresses, the gathered requirements might not cover every situation and technical partners will likely need to make some assumptions.

In order to ensure that the choices and assumptions made by partners are reasonable, some level of assessment is advantageous. Making the models publicly available and encouraging feedback from external researchers who wish to comment would be ideal.[59] However, this would not be possible in the context of ROXANNE due to the potential for commercial exploitation in the future, and the risks of criminal organisations viewing any publicly available code. As such, having technical partners to review the work of others within the consortium would be beneficial; further discussing the assumptions made in producing the models with LEAs would seem advantageous so that the platform is adequately tailored to their needs is created.

> *Requirement for technical work to be widely reviewed within the consortium and to ensure components fulfil LEA needs not yet possible to evaluate.*

[58] Silberzahn, R., "Many Analysts, One Data Set: Making Transparent How Variations in Analytic Choices Affect Results" *Advances in Methods and Practices in Psychological Science*, Vol.1, No.3, 2018 (hereafter: Silberzhan, 2018), pp.337-356.

[59] Silberzahn, 2018, pp.337-356, 353-354.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

A key privacy issue in the evaluation phase is that persons who test the ROXANNE platform will be interviewed. As mentioned above, data collection from people can create ethical harms where people are subject to interrogation.[60] However, it is important to differentiate interviews from interrogation. Interrogation involves the pressuring of individuals to reveal information they would not otherwise provide.[61] ROXANNE partners are aware of standards expected in research interviews and will plan interviews according to these standards. Partners will not pressure participants; they will be free to leave at any time, or not answer any questions that they do not feel comfortable answering.[62]

> *Requirement to plan interviews according to applicable standards of research ethics not yet possible to evaluate.*

> *Requirement for interviewees to not be pressured and treated according to research ethics standards not yet possible to evaluate*.

As with the requirement gathering phase, in order to ensure data quality and data integrity, partners should incorporate best practices when formulating interview questions and methods so that the data collected is relevant, accurate, complete, and reliable. Additionally, in order to ensure access to data for data-subjects, and the potential to fulfil their data rights, partners will only gather data from participants where they consent, and will use their consent as the legal basis for processing. These interviews will take place in the future and compliance with this requirement will be assessed once they have occurred.

> *Requirement for interview questions to enable data gathering that is relevant, accurate, complete, and reliable not yet possible to evaluate.*

> *Requirement to give data-subjects interviewed during the evaluation phase ownership over their data not yet possible to evaluate.*

In terms of transparency in this phase, the consortium should disseminate information about any setbacks or reservations towards the platform (as per their understanding) and how they dealt with it to create a platform which promises transparency and fairness but without compromising on it's efficacy to mitigate organised crime as envisioned by the consortium while developing this project. The project website could also have a 'Frequently asked questions' sections which addresses a summary of ethical and legal concerns related to the platform along with solutions. This is something that the legal and ethical partners are working towards.

> *Requirement for partners to be transparent about shortcomings of the platform during evaluation not yet possible to evaluate.*

> *Recommendation for the project partners to add a summary of ethical and legal concerns and solutions to the project website not yet possible to evaluate.*

At this stage, the technical partners should carefully evaluate the extent of the algorithmic transparency and judge whether it is sufficient as envisioned during the design phase. The need is to ensure that the functioning of algorithms, at least at a basic level, is clear to the LEAs. Further, it will be difficult for partners to evaluate the system if they do not adequately understand how it works. This is particularly relevant to the ROXANNE project, where different technological modules are being put together in order to build an integrated platform. Consequently, the technical partners should build the platform in such a way as to enable them to comprehend how the data-processing modules and operations work both individually, and in combination, in order that they can adequately evaluate the platform.

> *Requirement for technical partners to build the data-processing modules and overall platform in such a way that it can be understood and evaluated.*

[60] Solove, 2006, pp.491-504.

[61] Solove, 2006, p.500.

[62] See, for example, reference to interview standards in European Commission, Ethics in Social Science and Humanities, Horizon 2020 Guidance, October 2018. Avaialble at: https://ec.europa.eu/research/participants/data/ref/h2020/other/hi/h2020_ethics-soc-science-humanities_en.pdf

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

> *Requirement for technical partners to build the ROXANNE platform so that it is understandable to LEAs.*

Based on the analysis of field-test results and the evaluation of continuous testing results, the consortium will be in a position to enhance the ROXANNE platform 's operation and present end-users with a robust and reliable product that responds to their needs. However to this end, partners must treat equally, impartially and openly all the results and feedback received from partners and external stakeholders. The integration of the ROXANNE platform, its final platform setup, user interface and maintenance should reflect the different needs and issues signalled as the platform matures and its functionalities are evaluated in the context of the three milestone events (i.e. field tests). By adopting a fair, inclusive and comprehensive approach to the analysis of gathered input, partners will contribute to the development of a useful and feasible system for a diverse and wide range of end-users.

> *Requirement for partners to treat results and feedback equally, impartially, and openly not yet possible to evaluate.*

> *Requirement to build the platform to take into account different needs of potential users not yet possible to evaluate.*

In this phase, issues of individual wellbeing are limited to those relevant to project partners who are evaluating the outcomes of testing. Evaluating test data and responses to interviews/workshops would not seem to create significant risks toward individual wellbeing in the ROXANNE project. For example, there is no expectation that partners will need to deal with any distressing content from the field-tests, for example. It is also unlikely that societal or environmental wellbeing could be affected during evaluation as there are no effects that could come from this work which would have a material impact upon them.

> *Requirement to respect individual, societal, and environmental wellbeing during the evaluation phase, set to be completed.*

With regard to accountability, the consortium is collectively responsible to build a technically robust, legally compliant and efficient ROXANNE platform with acceptable errors rates, according to the project Grant Agreement provisions. Designated WP leaders are in charge of leading thematic and specialised efforts to this end, with the support of other partners. The end product should be achieved following the successful development and testing of the platform's individual components in the preceding steps (i.e. survey distribution, field tests). The integrated system's evaluation should confirm minimised levels of false positive/negative results, human errors, algorithm bias and malicious interference with the results. The evaluation results should be properly documented, shared with the EC and, where possible, with expert members of the stakeholder group to confirm their interpretation and the platform's sound functioning. Outside the research context, the subsequent users of the ROXANNE platform will be accountable for the use they make of the platform. Although still in its early stages, the project Exploitation Plan will agree on consortium-wide arrangements for exploiting project results, including acceptable IPR measures, in order to facilitate their uptake and use by potential end-users.

> *Requirement for the project partners to take responsibility for production of a platform in line with that agreed in the Grant Agreement.*

Phase 6: Use

As the ROXANNE platform is still in development, it is not possible to give a detailed assessment of how the platform will be used and the implications for its use on individuals and society. However, we can highlight some issues that might affect the use of the proposed platform. These will be further refined in D3.4 (Final report on compliance with ethical principles). Additionally, some issues related to use are larger than others and those which are subject to more detailed analysis are given sub-titles in the following text. Finally, as issues related to use are dependent upon the action of LEAs, the projects is not in a position to evaluate whether all ethical requirements are completed due to both the expected use occuring after the project, and operational LEA activities being beyond the control of the consortium, and so these are provided as recommendations.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

However, where issues arise from the expected use are relevant to the activities of partners during the project, these are still provided as requirements with reference to their completion or ability to be evaluated.

In discussing human agency, liberty, and dignity in the context of criminal network analysis technologies being used, there are two key areas for discussion. The first is LEA officer themselves: how does the use of advanced technology affect them and their role? The second area is the people who are subject to (or potentially subject to) analysis via these means, how does it impact on their ability to live their lives and act freely?

Alienation

With respect to the use of advanced technologies by LEAs, a major issue in relation to human agency and advanced technologies is automation bias. This is the process whereby human beings trust the outputs of machines more than themselves and so follow what the machine suggests, even when it goes against their own knowledge.[63] For Virilio, the speed of machines can overrun '*intelligent reflection*'.[64] A classic example is where drivers follow the instructions of their satellite navigation system into a dangerous situation.[65] Automation bias causes significant issues for human agency as the person making decisions is not acting with true agency, but is essentially acting as the agent of the machine. The implication of this is that, if affected by automation bias, the users of ROXANNE would be removing their own critical reflection about the outputs of the machine and the machine would, functionally, be acting as an autonomous agent itself. This is particularly concerning in the use of ROXANNE where, for example, an individual could be communicating with a criminal for innocent reasons but be included in the network analysis and potentially be included an intrusive investigation without an LEA officer taking a meaningful decision about whether they should be included .

For the human being using the machine , this can result in them being 'alienated' from their work;[66] feelings of alienation would be particularly relevant if some of the decision-making previously done by a human LEA officer is carried out by a machine. Where decision-making is delegated to machines, this can result in a de-skilling of the individuals who would otherwise have made those decisions; this is much the same as the de-skilling of factory workers through the introduction of mechanisation.[67] People using advanced technologies are particularly susceptible to alienation in this way as the very existence of better and faster technologies can '*discredit'* the use of slower methods, even where they involve human beings.[68]

The Law Enforcement Directive places a general prohibition on the use of automated individual decision-making.[69] However, Member State law can provide an exemption to this as long as there are appropriate safeguards and, at the very least, the possibility for human intervention.[70] Further, the use of automated decision-making on special category data is prohibited.[71] Still, the use of data-analysis technologies can still lead to automation bias even when they are not used for decision-making. For example, an LEA officer who might blindly follow an assistance tool as if it were making decisions rather than providing assistance; consider that a network analysis tool might potentially highlight persons of interest as an assistance tool, but, if this advice is blindly followed due to automation bias, then the tool is functionally being used for decision-making.

[63] See Skitka, Linda J., Kathleen L. Mosier and Mark Burdick, "Does Automation Bias Decision-Making?" *International Journal of Human-Computer Studies*, Vol.51, 1999, p.991.

[64] Virilio, Paul (trans Chris Turner), *The Information Bomb*, Verso, London 2000 (hereafter: Virilio, 2000), p.124.

[65] See, for example, Milner, Greg, "Death by GPS" *Ars Technica*, 2016. Available at: https://web.archive.org/web/20190602041744/https://arstechnica.com/cars/2016/05/death-by-gps/

[66] Automation meaning the use of automatic process to replace human cognition, in contrast to mechanisation replacing physical labour. Pyke, Magnus, *Automation: Its purpose and future*, Scientific Book Club, London, 1946, p.38.

[67] Marx, Karl (trans Martin Nicolaus), *Grundrisse*, Penguin, St Ives, 1993 (hereafter: Marx, 1993), p.701

[68] Virilio, 2000, p.123.

[69] Art.11 (1), European Parliament and Council, Directive (EU) 2016/680 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, OJ L 119/89, Vol.59, 4 May 2016 (Law Enforcement Directive, hereafter: LED).

[70] Art.11 (1), LED.

[71] Art.11 (2), LED.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

For LEAs, this can mean that the individual officer who would otherwise have been deployed to monitor suspects is no longer needed, [72] or becomes merely an overseer of a machine[73] that is carrying out the real work.

For LEA officers, this de-skilling could result in the loss of their ‘intuition’ about what is suspicious in criminal investigations; and potentially an atrophy of moral skills in deciding what the right course of action is in relation to surveillance operations.[74] Considering that intuition of LEA officers is very useful in investigations,[75] and LEA officer can be seen as ‘*societal moral agents*’ (i.e. embodying the moral virtues of a society),[76] it is imperative that the use of new criminal network analysis platforms do not damage either of these aspects. A third form of de-skilling is where the user becomes less able to determine when a technological system has made a mistake, and given that surveillance and analytics technologies will generate both false positives and false negatives, this ability to assess the outputs of a system remains important.

One solution to dealing with both automation bias and the alienation of people from their work is to place the human being at the very centre of critical decision-making. This means that the ROXANNE platform requires human input across various stages of its use, rather than automating specific activities. This is an emerging concept in military thinking where it is referred to as ‘human-machine teaming’.[77] It has been popularised by players of ‘advanced chess’, where each player has a computer analysing potential moves but the player chooses which moves to make according to their strategy.[78] Generally, this approach requires using a computer systems for tasks that it excels at (i.e. searching and sorting large amounts of structured data and deterministic analysis), and having human beings perform the tasks they are good at (i.e. comprehending complex and unstructured data and non-deterministic analysis).

In the context of ROXANNE, for example, this could involve building the platform in such a way that LEA users are required to decide upon what investigative data should be analysed by the platform and what it should look for. The system could then analyse phone or video recordings and search for instances that an LEA officer instructed it to. If the system finds these instances and highlights them to the officer, then the LEA officer should determine what is useful to the investigation and justify why this is and why they choose to investigate them further; a key aspect of this for ROXANNE would be related to the use of network analysis and which individuals in the communication network of a criminal should be subject to further investigation. By framing the human-machine relationship in this way, it places the human being at the centre of the ROXANNE platform. This means that LEA officers must engage directly with the key issues arising investigations and the use of data-analysis platforms during those investigations, it also means that they can apply the required moral and legal standards to the use of ROXANNE in their investigations. The need for human beings to engage directly with decision-making should be made clear to end-users during training. Consequently, the consortium should reflect the need for human beings in decision-making in the promotion and exploitation of the system; the consortium partners should not encourage the problematic view that the tool does ‘everything’ in the analytic process.

[72] Marx, 1993, p.695

[73] Marx, 1993, p.705

[74] Brownsword, Roger, “In the year 2061: from law to technological management” *Law, Innovation and Technology*, Vol.7, No.1, 2015, pp.1-51, 35.

[75] See, for example, Wright, Michelle, “Homicide Detectives’ Intuition” *Journal of Investigative Psychology and Offender Profiling*, Vol.10, 2013, pp.182-199; Akinci, Chris and Eugene Sadler-Smith, “‘If something doesn’t look right, go find out why’: how intuitive decision making is accomplished in police first-response” *European Journal of Work and Psychology*, Vol.29, No.1, 2020, pp.78-92.

[76] Dirikx Astrid, Jan Van den Bulck, and Stephan Parmentier, “The Police as Societal Moral Agents: “Procedural Justice” and the Analysis of Police Fiction” *Journal of Broadcast and Electronic Media*, Vol.56, No.1, 2012, pp.38-54; Goldsmith, Andrew J., “Policing’s New Visibility” *British Journal of Criminology*, Vol.50, pp.914-934; Sunshine, Jason, and Tom Tyler, “Moral Solidarity, Identification with the Community, and the Importance of Procedural Justice: The Police as Prototypical Representatives of a Group's Moral Values” *Social Psychology Quarterly*, Vol.66, No.2, pp.153-165.

[77] See, for example, UK Ministry of Defence, *Joint Concept Note 1/18 Human-Machine Teaming*, Development, Concepts and Doctrine Centre, Wiltshire, 2018, pp.39-43.

[78] Kasparov, Garry, *Deep Thinking*, John Murray Publishers, London, 2018, pp.244-246.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

> *Requirement for technical partners to build the ROXANNE platform in such a way as to require LEA officers to make all decisions, not yet possible to evaluate.*
>
> *Requirement for training materials to highlight that the LEA users should treat the ROXANNE platform as an assistive tool, not yet possible to evaluate.*
>
> *Requirement for promotion and exploitation of the platform to avoid implications that the platform can automate decision-making, not yet possible to evaluate.*

Professional ethical drift

Many professions and fields of practice have formalised codes of ethics and/or conventional ways of behaving appropriately in that field. For example, LEA officers may have taken explicit oaths, but are also likely to subscribe to a less explicit set of ethical values built up in their organisations over time. The adoption of technological systems can put pressure upon these codes of practice, influencing or undermining particular values that are important to a profession, and changing the way that work is done in the field, in ways which may not align with those values. LEA professionals are important stakeholders for ethics in ROXANNE and the project should endeavour to understand the professional ethical values that ROXANNE technologies should be able to support.

> *Requirement for ROXANNE researchers to try and understand the informal professional needs not yet completed.*

Dehumanisation

For individuals who might be placed under surveillance, a key issue related to human dignity is that they may no longer be treated as people whose data is being analysed, but as mere data-points. For Kantian ethics, this would be an affront to the concept of human dignity, where the respectful treatment of human beings is an end in itself and treating individuals as mere objects violates their dignity.[79] Philosophical literature suggests that the treatment of people as machine-like is a process of objectification and dehumanisation.[80]

In the situation of analysing data relating to individuals, as in the case of ROXANNE, dehumanisation does not relate to the people who are investigated by LEAs being treated as machines but being treated as part of a machine because data about them forms part of the functioning of the platform. Whilst this type of dehumanisation happens with the use of various technologies, ROXANNE poses a particular issue as it is not just an individual whose data is analysed, but their communication networks as a whole that can be analysed (given access to these data). This increased scale of data analysis means that entire social groups localised around criminal suspects could be dehumanised. This does not mean to suggest that the use of ROXANNE would necessarily result in the dehumanisation of entire social groups resulting in large-scale discriminatory effects and potentially atrocities.[81] However, the existence of dehumanisation could contribute to dehumanisation of social groups if, for example, members of a criminal organisation are predominately from a minority group.

We see some similar situations with the treatment of minorities by police today.[82] Yet, the effect of this could be that not only are people from these groups subjected to intrusive surveillance more easily than peers from a majority group, but that by continuously engaging in network analysis and generating more surveillance subjects from these networks, the effect is mass-surveillance of minorities. Consequently, this reinforces the

[79] Kant, Immanuel (trans. H.J. Patton), *The Moral Law*, Hutchinson's University Library, London, 1947, pp.96-97.

[80] Haslam, Nick, "Dehumanisation: An Integrative Review" *Personality and Social Psychology Review*, Vol.10, No.3, pp.252-264.

[81] Murrow, Gail B and Richard Murrow, "A hypothetical neurological association between dehumanisation and human rights abuses" *Journal of Law and Biosciences*, Vol.2, No.2, pp.336-364.

[82] See, for example, Butler, Paul, "The policing of black Americans is racial harassment funded by the state", the Guardian, 6 June 2018. Available at: https://www.theguardian.com/us-news/2018/jun/06/america-police-called-on-black-people-everyday-racism

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

need to develop ROXANNE according to EU and national laws, and to only exploit the platform to end users who are expected to abide by the law. Thus, risks of mass surveillance should be avoided (also see D10.16 Report on the risks of misuse and mass surveillance); indeed, ROXANNE is intended to streamline analysis of data that is already lawfully collected and not to increase the surveillance capacity of LEAs.

> *Requirement for partners to ensure the ROXANNE platform is developed according to applicable legal standards, not yet possible to evaluate.*

> *Requirement for partner to avoid exploitation to customers who pose a risk of engaging in unlawful activity, not yet possible to evaluate.*

Chilling effects

Another potential impact of ROXANNE on the individuals who will be subject to criminal network analysis is the potential for its use to interfere with negative liberty (meaning the freedom to do things without interference), in particular political freedoms. Surveillance technologies that already exist are known to create 'chilling effects',[83] meaning that people who know or suspect they will be surveilled act in more restrained ways to what they would otherwise do if they were not subject to surveillance.

A potential effect of the ROXANNE platform is that the impact of criminal network analysis does not just affect the individuals whose data is analysed, but also that of the people whom they communicate with. Thus, where people perceive their friends and family to be at risk of surveillance, or data-analysis by LEAs using ROXANNE, due to their actions, they would likely be less inclined to participate in activities that could raise the interest of LEAs. If activities that are affected by 'chilling effects' are criminal, then the ROXANNE platform would have a greater deterrent effect on would-be criminals than systems that are already in use. This would seem to be a positive effect towards preventing crime.

However, this deterrent effect can be negative where it prevents people engaging in innocent behaviours that they believe will attract the attention of LEAs.[84] This is especially concerning in countries that suppress political opposition and the deterrent effect interferes with their perfectly innocent political activities and freedom of expression. As mentioned in D10.16 (Report on the risks of misuse and mass surveillance), the ROXANNE platform will not be exploited to countries with poor track-records of complying with human rights law. Further, as mentioned above, including a decision-making mechanism in the platform that requires LEA officers to evaluate data they are intending to analyse should prevent the ROXANNE platform from being used in an arbitrary way.

> *Requirement for ROXANNE not to be exploited to LEAs with a poor track-record of complying with human rights law, not yet possible to evaluate.*

Issues of robustness and safety are significant in terms of use, as it is the crucial moments where effects might be created for the public if ethical risks manifest. In terms of safety and security, there are risks that an insecure platform could be attacked by criminals; if they were to gain access to the platform this might not only disrupt investigations, but also ongoing criminal trials and, potentially, previously secured convictions through evidence tampering. As such, it is imperative that LEAs only use the ROXANNE platform on secure systems.

> *Recommendation for LEAS to only use the ROXANNE platform on secure systems.*

Interpretation of results

However, other aspects related to the accuracy, reliability, and precision of the system, and how this is perceived, can generate significant ethical risks during the use of the platform. A significant issue with the use of algorithmic processes to assess real life activities is the fact that it can only comprehend quantitative methods. As Malik writes, we may be able to engage in many mathematical analyses of different situations or

[83] Solove, 2006, 477-560, p.487.

[84] Stoycheff, Elizabeth, "Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring", *Journalism & Mass Communication Quarterly*, Vol.93, Issue 2, pp.296-311.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

individuals, but these types of analysis do not lend themselves to understanding what they mean.[85] The ROXANNE platform might highlight a particular activity as unusual but cannot explain why.

For example, if there is an increased frequency of phone calls between a known criminal and their family, one interpretation of this information could lead to a view that they are a familial criminal organisation and another interpretation could be that there is an ongoing family emergency. There is, therefore, a risk that an end-user could misunderstand the outputs of the platform and, in this example, expand their investigation to family members. Whilst LEA policies would normally result in the discarding of data that is not relevant to the investigation, the initial intrusion into an innocent persons private life is ethically problematic. It might be proportionate in a criminal investigation, but is still regrettable.

Consequently, the inability of the platform to provide meaning for its outputs highlights the need for human beings to critically evaluate them prior to acting on the results. Considering the speeds and scales at which advanced technologies work, a lack of critical reflection on platform outputs could result in a significant number of people being unnecessarily investigated.

> *Recommendation for LEAs to critically evaluate platform outputs in terms of their accuracy, reliability, and precision prior to acting on them.*

Further, the use of machine learning models to discover knowledge about criminal organisations cannot be used to analyse the qualitative reasons about what makes them, and their members, criminal. The use of other metrics typical of criminal behaviours can be a useful indication of, or proxy for, criminality, but never a true representation of it.[86] For example, particular patterns of behaviour might be measurable and associated with criminal activity but are not definitive; a recording of a known criminal using apparent code words might indicate their participation in hiding their purchase of contraband, or might be hiding a surprise present for their spouse. If the outputs of ROXANNE suggest that a suspect has acted in a way typical of criminals, then that is all that the results mean; it is not a determination of criminality. As such, the outputs of platforms like ROXANNE are always an estimation and, therefore, require the presence of a human beings to assess them, what they suggest about a suspect and how they should impact on the investigation.

> *Recommendation for LEAs to not treat ROXANNE outputs as conclusive, or indicative of criminality.*

This point is part of a wider issue of neglecting the "knowledge infrastructure" from which data used for analysis arises – the complex set of people, practices, technologies, institutions and relations that produce data in a particular context.[87] To treat data as if interchangeable, and free of context is to miss the way that data comes from a particular place and a particular context. It is the responsibility of the ROXANNE consortium as users of data to understand its situated nature, and make end-users aware of this in terms of the data used to train models but also make them aware of how the use of their own data will affect the outputs of the platform. In practice this might mean considering, for example, how people come to be included in police data sets (or be excluded from them), and what social dynamics might be in play in this. In research terms, this is also an issue that affects the generalisability of any analytic model. Thus, when using the platform, LEAs should consider what information is available about context from any open data sets that we use in the project. In order to explain the appropriate context for using the platform, this information should be provided to potential customers before sale, and the consortium will likely have to do some "translation" work, to make this contextual information meaningful.

> *Requirement for partners to make potential customers aware of the context in which the models were built, and how this affects the outputs of the platform not yet possible to evaluate.*

Where critical reflection is missing, this can sometimes lead users of system to view the world through the affordances of the analytical tool. For example, on social media people can see the popularity of a person

[85] Malik, Momin M., "A Hierarchy of Limitations in Machine Learning" *arXiv.org*, 29 February 2020 (hereafter: Malik, 2020). Available at: https://arxiv.org/abs/2002.05193, pp.6-8.

[86] Generally, see DeVellis, Robert F., *Scale Development*, 4th edition London, SAGE, 2016; Malik, Momin M., 2020, pp.8-12.

[87] Borgman, C., Big Data, Little Data, No Data: Scholarship in the Networked World, Cambridge MA., MIT Press, 2015.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

through the number of people they interact with online rather than how people feel about them.[88] In a similar way, it might be possible for some users of ROXANNE to view the level of criminality a person engages with through the prism of the number of criminal acquaintances they have, rather than their actual behaviour. Owing to the power asymmetry of LEA officers in relation to the public, such privileging of knowledge from LEA officers could lead to 'epistemic violence' where harm is caused through not appreciating other ways of 'knowing' (e.g. that someone might know a lot of criminals because they are friends, and not because they are engaged in criminality together).[89] Additional training of users to make them aware of this issue and forcing users to make substantive decisions in the decision-making process might move people from this vein of thinking into actually evaluating the criminality of suspects, for example.

> *Requirement for the ROXANNE training provision to include information about the meaning of ROXANNE outputs not yet possible to evaluate.*

Use of data

During actual investigations potentially using the ROXANNE platform, it is inevitable that the privacy of criminal suspects and their associates, and potentially the privacy of innocent people, will be violated during an investigation. As mentioned above, infringement on privacy for legitimate law enforcement purposes with constraints of proportionality, an appropriate legal framework, and effective oversight, is generally regarded as acceptable.

The ability of the ROXANNE platform to recognise persons whose data is gathered by surveillance methods such as CCTV or wire-taps is somewhat dependent upon the quality of the images, or voice recordings, for example. Consequently, if these technologies are old, or have low-resolution, then the ability of the ROXANNE platform to compare images or voice samples against those from a database is limited. This would clearly raise an issue in terms of accuracy, completeness, and reliability of data. Thus, technical partners should determine an appropriate minimum standard for which data is acceptable to be used with the ROXANNE platform. Further, LEA officers should be cognisant of the potential effects that poor-quality data could have for the results when they review them.

> *Requirement for technical partners to determine a minimum level of data quality that the platform can reliably be used to analyse, not yet possible to evaluate.*
>
> *Recommendation for LEA officers to be cognisant of the limited utility and potential for erroneous outputs when using poor quality data.*

During the use phase, a key issue is access to data. This is particularly relevant due to the sensitive nature of the data that is analysed in LEA investigations. These data should only be accessible by the investigators that are working on the case at hand; generally, it would seem to be a disproportionate invasion of privacy if, for example, officers not investigating the case began to access these data. However, there may be situations where this is appropriate and ROXANNE provides a key example. For example, if LEAs are investigating two organised crime activities in separate investigations, it might become apparent that some of the suspects in each case are the same; this could suggest that either some of the suspects are well-connected in criminal activities or the separate investigations are looking at the two parts of the same organised crime group. Using ROXANNE to analyse the two datasets and visualise the criminal networks might be a way of quickly showing whether the two criminal activities are linked.

To use ROXANNE in this way could be very useful for LEAs. But, if it were used to do this without proper reason or in the hope of finding connections in seemingly unconnected investigations (i.e. a 'fishing expedition'), this would seem to be an illegitimate use of the technology. Therefore, it would seem appropriate

[88] Malik, Momin M, and Jürgen Pfeffer, "Identifying Platform Effects in Social Media Data" *Proceedings of the Tenth International AAAI Conference on Web and Social Media (ICWSM 2016)*, pp.241-249, 247. Available at: https://www.aaai.org/ocs/index.php/ICWSM/ICWSM16/paper/view/13163/12744.

[89] Spivak, Gayatri Chakravorty, "Can the Subaltern Speak?", in Cary Nelson and Lawrence Gossberg (eds.), *Marxism and the Interpretation of Culture*, Macmillan Education, London, 1988, 280-283.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

for all personnel using ROXANNE to log their use of the system, and their reasons for using it in a particular way. These reasons should be evaluated by independent individuals who are separate from either investigation, such as a senior officer not involved in detective work.

> *Recommendation for LEA investigators to generally restrict access to data to the investigation team, and only allow access to other investigators for legitimate reasons.*

Logging the use of ROXANNE provides clear links with accountability, as it identifies individuals who can be held responsible for the actions that take place using ROXANNE. Further, this can also add to a culture of respecting privacy in organisations; where individuals know they must explain their actions regarding personal data, this would, presumably, cause people to consider whether they need to engage in the activity in question. Technology design should support this through the use of user-interface patterns – for example, requiring a user to log a rationale for using the platform before opening it, or appending the rationale as meta-data to the outputs of an analytic process.

> *Requirement for technical partners to incorporate mechanism for logging uses of the ROXANNE platform not yet possible to evaluate.*
>
> *Recommendation for LEA officers to log their uses of the ROXANNE platform, and the reasons why.*
>
> *Recommendation for uses of the ROXANNE platform to be evaluated by persons independent from investigations.*

With regard to data-rights and ownership, the LED provides for fewer data rights than the GDPR as mentioned. It is assumed by the ROXANNE partners that end-users will use the platform lawfully and so any denial of data-subject rights will be legitimate. With respect to ownership, it is important that LEAs own data gathered during surveillance operations as it is, by its nature, sensitive and therefore requires handling processes that LEAs are experienced with. Consequently, such data should remain with LEAs and, where necessary, the court system.

> *Recommendation for sensitive LEA data to remain with LEAs.*

Public awareness about the scope and implications of ROXANNE

Transparency is a particular issue in today's technology-filled world. Citizens are increasingly being watched and tracked in the name of public safety and security.[90] The ability of governments and organisations to keep people's activities under surveillance has never been greater.[91] While law-abiding citizens often understand the need for enhanced security measure, many fear that in a world of aggregated data, which includes varied sources such as credit card purchases, web browser histories, healthcare records, personal information, and more will be assembled to form gigantic data footprints about individuals to aid in state surveillance.[92] Hence, it is important to focus on people's knowledge of and familiarity with uses of their data, and in, the case of ROXANNE, biometric technologies and biometric recognition. Specifically, this should consider their awareness of the possible uses of such systems in the fight against crime and terrorism. Whilst many of the tools and practices used by LEAs for these purposes are lawful, the ability to misuse these technologies for nefarious purposes is, for King, the very basis of distrust between the public and the LEAs in terms of technology use. [93]

[90] Draper , Robert, "They Are Watching You—and Everything Else on the Planet", Nationalgeographic.com, 2018.Available at: https://www.nationalgeographic.com/magazine/2018/02/surveillance-watching-you/;Dans, Enrique, "Are we sliding inevitably into a surveillance society?", Medium .com, 2015. Available at: https://medium.com/enrique-dans/are-we-sliding-inevitably-into-a-surveillance-society-5c847f22fe39; Feldstein , Steven , "Global expansion of AI surveillance", carnegieendowment.org, 2019. Available at: https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847

[91] K.N.C, "Surveillance is a fact of life, so make privacy a human right", Economist.com, 2019. Available at: https://www.economist.com/open-future/2019/12/13/surveillance-is-a-fact-of-life-so-make-privacy-a-human-right

[92] King, Rawlson, "People fear the future of technological surveillance", Biometricupdate.com, 2012. Available at: https://www.biometricupdate.com/201211/people-fear-the-future-of-technological-surveillance

[93] Douglas Heaven,Will, "Predictive policing algorithms are racist. They need to be dismantled", Technology Review, 17

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635.

These tools pose ethical challenges irrespective of the results that they produce. Hence transparency is one of the key aspects to be kept in mind while designing such a platform.

There are a variety of ways to tackle this. To begin with, it is imperative that the public is aware of the scope of work and implications of this platform for the LEAs to be able to implement this platform. This includes aspects of data collection, processing of information, plausible downsides of the platform, use of technologies, certainty of results and promised supervision to avoid any misuse of the platform; of course, this needs to be managed with the sensitivities of performing police work and the need to not provide too much information to the public in case it benefits criminals in avoiding detection. In case of a lack of information on the above aspects, this platform might be thought of as a tool meant for mass surveillance and hence might not be accepted as widely.

Recommendation for LEAs to be open about their use of ROXANNE, and supervision of this, as much as possible taking into account operational needs.

Algorithmic transparency is important in the use of data-analysing platforms, especially in law enforcement. As LEA activities are inextricably linked to the criminal justice system, LEA use of these technologies is subject to court scrutiny. If the ROXANNE platform is a 'black box', and it's functioning is unknowable, this can pose a serious risk to due process, and accountability. Indeed, some authors suggest that 'black box' algorithms should be prohibited in '*high-stakes*' areas, such as criminal justice, and, at a minimum, it should be possible to subject such systems to '*public auditing, testing, and review, and* [...] *accountability standards*'.[94]

Requirement for the functioning of the ROXANNE platform to be knowable in order that it can be subject to public analysis and accountability measures, where necessary.

In order to make sure that the people feel that their rights will not be hampered by implementation of such a platform, it is important to spread awareness about the intended use of the platform discussing both pros and cons of the platform. The use of marketing collaterals (dissemination materials) [95] should be made to reach to the right audience using avenues such as global conferences, webinars, blogs, social media, newsletter etc. There should be a proactive attempt to discuss the possible unintended results of this platform or even an attempt to understand any other reservations citizens have with respect to this platform. A survey or a focus group discussion with volunteers could result in some useful insights which can then be leveraged in the design stage of the platform.

Requirement to gather feedback on potential issues that could be generated by use of the ROXANNE platform, not yet possible to evaluate.

Studies have shown that citizens' in developed countries, such as the US, are more comfortable with the use of biometrics in places of high-security requirements such as the airports or banks.[96] We can draw from this that the public is more open to the idea of use of biometrics data collection and analysis if they understand what it is for and how it protects them. Hence, it is utmost important to be vocal about the problems ROXANNE would solve and how it is going to help LEAs maintain peace and harmony in a society.

Requirement for the ROXANNE consortium to explain the intended platform and its uses in publicly available dissemination materials, not yet possible to evaluate.

July 2020. Available at: https://www.technologyreview.com/2020/07/17/1005396/predictive-policing-algorithms-racist-dismantled-machine-learning-bias-criminal-justice/

[94] Selbst, Andrew, and Solon Barocas (eds., AI Now 2017 Report, AI Now Institute, 2017. Available at: https://ainowinstitute.org/AI_Now_2017_Report.pdf

[95] Katai , Robert, "Marketing Collateral: From Definition to Examples", Robertkatai .com, 2018.Available at: https://robertkatai.com/marketing-collateral/

[96]Ibia.org, "Recent Opinion Surveys on Public Perceptions of Biometrics", Ibia.org, 2016. Available at: https://www.ibia.org/download/datasets/3372/Public-Perceptions-of-Biometrics-opinion-surveys%20.pdf

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

Clarity on protection of personal data

One of the primary apprehensions with respect to a platform such as ROXANNE which analyses biometric data of people is the misuse of this personal data to compromise the privacy of data subject.[97] As per the GDPR, biometric data falls under the category of "special categories of personal data" and its processing is prohibited (in the absence of particular exceptions)[98]. However, it is important to note that, during law enforcement activities, LEAs follow the Law Enforcement Directive (LED) which is a regulation parallel to GDPR and deals with the processing of personal data by LEAs for the '*prevention, investigation, detection or prosecution of criminal offences*' – which falls outside of the scope of the GDPR.[99] The LED allows LEAs to process sensitive personal data such as biometrics for law enforcement purposes.[100]

In order to process and collect the data ethically while ensuring transparency, it becomes imperative to comply with legal requirements. These requirements are present in the LED to ensure accountability,[101] transparency[102] and fairness[103] without compromising on needs of law enforcement agencies to maintain law and order in society. Some of the provisions of the LED include need to categorise individuals (i.e. witness, convict, suspect, victim etc.), before the processing of personal data takes place. Another interesting article as a part of LED is based on Article 11 "Automated individual decision-making", which provides safeguards for individuals against the risk that a potentially damaging decision is taken by solely automated means, i.e. without human intervention. This processing can only be done while ensuring the protection of the rights and freedoms of the data subject. Further, as per Article 24, to ensure accountability, the LEAs would be required to maintain relevant documentation to prove compliance with principles and responsible processing of personal data. Failure to abide by these legal rules could lead to a sense amongst the public that LEAs operate beyond the law, potentially leading to feelings of mistrust and fears of mass surveillance. Consequently, having LEAs abide by the law reinforces trust amongst the public, especially when investigators are dealing with sensitive issues such as biometric personal data.

Recommendation for LEAs to process data in accordance with the LED.

All in all, even with thoughtful safeguards in place, just processing data ethically and lawfully is not enough, the public should be made well aware of it too. By clearly providing details about why, how and where an organisation is collecting and storing biometric data (wherever possible), organisations can build trust and assure people that their data is being used in secure way [104].

Recommendation for LEAs to be open about their policies for processing personal data.

Effects of biased data

When considering the ROXANNE platform's actual implementation, beyond the project research and development phase, potential risks associated with the system's misuse have implications on non-discrimination and fairness requirements. The potential implications of biased data being used during the development of the platform, and the possible effects of this have already been noted above.[105] However, it is also clear that end-users are products of their societies, and biases in those societies can, therefore, affect the

[97] Thalesgroup.com, "Biometrics: definition, trends, use cases, laws and latest news", Thalesgroup.com, 2020. Available at: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics
[98] Art.9(2), GDPR.
[99] Art.1(1), LED
[100] Art.10, LED
[101] Art.4(4), LED
[102] Arts.24 and 25, LED
[103] Art.4(1), LED
[104] Wood, Simon, "Biometric authentication: The importance of transparency and trust", IT Pro Portal, 2020. Available at: https://www.itproportal.com/features/biometric-authentication-the-importance-of-transparency-and-trust/
[105] See, for example, Benjamin, Ruha, Race After Technology, Polity Press, Cambridge 2019, p.165; Valentine, Sarah, "Impoverished Algorithms: Misguided Governments, Flawed Technologies, and Social Control" Fordham Urban Law Journal, Vol.46,, No.2, pp.364-427, pp.370-371

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

work of LEAs.[106] Thus, the intention of the consortium to build a platform that requires human decision-making at each key steps presents key points where societal biases can affect use of the platform. Babuta and Oswald note that specific guidelines for operations using data-driven technologies should be provided to investigators, and these should complement existing professional practice and approaches. Ethical and legal partners will explore the potential of highlighting issues such as potential discrimination in the electronic decision-making platform to be developed in T3.6 (Development of a decision-making mechanism).

> *Recommendation for LEAs to update training materials to highlight potential discrimination issues present with end-users.*

> *Requirement for ethics and legal partners to evaluate decision-making mechanism for mitigating discrimination issues, not yet possible to evaluate.*

In the event that the developed solution lands in the wrong hands (i.e. non-authorized users, authoritarian regimes), it could be used against innocent people or to target vulnerable segments of the population such as migrants or minors. The consortium is aware and considering seriously such threats and their consequences as identified in deliverable D10.16 (Report on the risks of misuse and mass surveillance). To this end, in addition to acceptable IPR arrangements and commercialisation strategy, the project Exploitation Plan will include some specific mitigation measures to diminish the potential occurrence of technological abuse through sound commercialisation practices i.e. due diligence checks, mandatory risk assessment, “no resale” clause (i.e. prohibiting the buyer from reselling the platform) in contracts, centralised software licence control, etc.

> *Requirement for exploitation process to avoid provision of ROXANNE technologies to non-authorised users and authoritarian regimes, and follow the exploitation guidelines, not yet possible to evaluate.*

Effects on individuals

The effects of having surveillance data analysed by LEAs can cause issues for individual wellbeing. When people are aware that they are under surveillance, this can create negative feelings and anxieties about the revelation of intimate information to unknown individuals and what they might do with it.[107] However, it is unlikely that in a criminal investigation, people will be made aware they are under surveillance by LEAs who have access to ROXANNE as this would likely result in the suspects changing their behaviours to hide their criminality.[108] As such, it is unlikely to be a significant issue with the use of ROXANNE. The revelation of being under investigation, if an investigation is later revealed (for example in court) might trigger some individual wellbeing issues, but these are comparable to other police investigations. Some jurisdictions may have an obligation to inform suspects of an investigation when it has been concluded – the ROXANNE project should consider how it can support this process where appropriate. There may also be collective welfare implications for the public knowing that LEAs have and use the types of tools contained within ROXANNE; as mentioned above, this could have an impact on public trust in LEAs.

> *Requirement for ROXANNE partners to consider the implications for persons finding out that they have been analysed by the platform, not yet possible to evaluate.*

[106] Williams, Patrick, and Eric Kind, Data-driven policing: The Hardwiring of Discriminatory Policing Practices Across Europe, European Network Against Racism, 2019. Available at: https://www.enar-eu.org/IMG/pdf/data-driven-profiling-web-final.pdf; Chowdhury, Areeq, Unmasking Facial Recognition, WebRoots Democracy, 2020. Available at: https://webrootsdemocracy.files.wordpress.com/2020/08/unmasking-facial-recognition-webroots-democracy.pdf, pp.8-9.

[107] See, for example, Stuart, Avelie, and Mark Levine, “Beyond ‘nothing to hide’: When identity is key to privacy threat under surveillance” *European Journal of Social Psychology*, Vil.47, No.6, October 2017, pp.694-707.

[108] Foucault, Michel (trans. Alan Sheridan), *Discipline & Punish*, 2nd Edition, Vintage Books, New York, 1995 (hereafter: Foucault, 1995), p.201

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

Privacy of personal lives and relationships

From the Foucauldian perspective, surveillance is not specifically about observing what a person is doing but about who they are and how that is observed across their life and in their relationships.[109] In this sense, the analysis of voice intercepts or surveillance camera recordings might reveal that a person has carried out criminal activities, for example evidencing someone discussing the purchase of illicit products and then showing them buying illegal goods. However, through the addition of network analysis and this revealing how people relate to, and interact with, other people, ROXANNE provides insight beyond what people do and into who they are as a person. As such, this is a greater invasion of privacy that that associated with conventional technologies as it exposes more information about their lives and relationships.

Whether this can be ethically justified depends upon a proportionality assessment. For example, viewing the recordings of a surveillance camera covering a crime is likely to be proportionate as it is the behaviour of the offender that is at issue and the invasion of their privacy is relatively small; the surveillance recording is watched only for as long as it takes to observe the crime and identify the suspect. If it is difficult to identify the offender from the tape, and the crime is serious, it might also be proportionate to subject it to technological analysis such as facial recognition in order to further the investigation and apprehend the offender.

From this perspective, it would not seem proportionate to explore who the person is as a human being in order to discover if they have committed criminal acts. Investigating the social relations a person has does not *prima facie* appear relevant to criminal investigations. The acts of a bank robber are relevant to a criminal investigation, who they are friends with is not. As such, it is the activities of a person that should be investigated, not who they are.

However, this ignores to key issues: first, that in order to sufficiently understand what a person does, it can be necessary to understand who they are; second, modern society has an interconnected nature and this includes organised crime groups, who can be understood as networks.[110] Regarding the first issue, where a crime takes place and the perpetrator is unknown, it might be necessary to investigate who suspects are in order to include or exclude them from further investigation. Whether this is proportionate would depend on the crime, it would seem disproportionate to look into the background of every person who visited a shop to trace a petty thief; it might not seem disproportionate to do this if a terrorist left a bomb in the same shop.

Turing to the second point, organised crime groups are often good at hiding their criminality through using others to do their bidding or adapting their operations to avoid the interest of law enforcement, such as using 'secure' communication technologies.[111] As such, to uncover criminality and prosecute offenders, law enforcement is required to explore deeper into the lives of suspicious individuals in order to find evidence of criminal activity. Of course, in order to begin an organised crime investigation, law enforcement must have some way of finding those to look at more closely. Platforms like ROXANNE, that can evaluate large amounts of data for points of interest, could be useful for highlighting points of potential criminality where additional examination could be fruitful.

> *Recommendation for LEA officers to consider the proportionality of using analytical tools in the ROXANNE platform during investigations.*

Part of the necessary evaluation of proportionality must include the potentially vast number of innocent individuals who could be caught up in network analysis. Gathering data on them as a side-effect of investigating a suspected criminal should be minimised as much as possible in the first instance, and only where it is unavoidable should it be considered. It should only go ahead where it is proportionate to the

[109] Foucault, 1995, p.208; Stoddart, Eric, "A Surveillance of Care: Evaluating Surveillance Ethically" in Kirstie Ball, Kevin D. Haggarty, and David Lyon (eds.) *Routledge Handbook of Surveillance Studies*, Routledge, London, 2012, pp.369-376, 372.

[110] See, for example, Diviák, Tomáš, "Sinister connections: How to analyse organised crime with social network analysis?" *Philosophica et Historica*, Vol.2018, No.2, 2018, pp.115-135.

[111] UK Government, *Serious and Organised Crime Strategy*, 2018, pp.1-2, 14-15. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752850/SOC-2018-web.pdf

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

criminality under investigation. ROXANNE partners should consider how the analytic capabilities of the platform will be presented to the user, and how they might practically integrate with existing investigative procedures, as this could make a big difference to proportionate use of the ROXANNE tools.

> *Requirement for ROXANNE partners to evaluate how data analysis will be presented to end-users so that it complements LEA procedures and assessing proportionality of decisions in investigations, not yet possible to evaluate.*

Viewing technology on the societal level

For some theorists, the impact of technology can be seen best on the societal, rather than individual, level.[112] In this tradition, Foucault suggests that widespread use of surveillance can create a '*discipline-mechanism*' that enables more efficient use of state power across society through making people more subservient to police actions, in contrast to individual and separated exercises of surveillance.[113] For Foucault's 'discipline-mechanism' to exist, it does not necessarily require mass surveillance to be occurring, but can be present where there is a significant number of surveillance methods such that people can be observed at many different instances;[114] this does not quite reach the level of panopticism where all people could be observed at all times.

However, the fact that the proposed ROXANNE platform can bring together and simultaneously analyse different types of investigative data from surveillance systems could mean that it goes beyond individual and separated uses of surveillance and begins to approach a 'discipline-mechanism'. If this occurs it would be a negative development for society, as the subjection of citizens to state power reduces the autonomy and freedom that they have. For Foucault, the domination of citizens by the state creates additional surplus power for the state.[115] Whether this is abused in the vein of mass surveillance or not, the fact that ROXANNE could generate greater power for the state presents heightened risks of abuse.

Foucault suggests that a solution to this is to instil democratic control over surveillance technologies.[116] As the ROXANNE consortium will not exploit the platform to authoritarian regimes (see D10.16 Report on the risks of misuse and mass surveillance), it can be expected that use of ROXANNE will be subject to political oversight by persons democratically voted to represent the public.

The debates necessary for effective democratic control can be informed by having wide ranging consultations and disseminating the results. The ROXANNE partners have conducted a global survey in T2.1 (Collection of end-user requirements), will gather feedback on the use of the technology in WP8, and will collect views of ethical, legal, and societal issues in WP3. Some of the results will be disseminated, and some of the recipients will include policy-makers (see, for example, T3.3 Fundamental rights below).

> *Requirement for the ROXANNE platform to gather and disseminate wide-ranging views, not yet completed.*

Further, it would be useful for the debates within LEAs about whether they should, or how they should, use particular technologies could be explored by their own stakeholder groups. For example, consulting with citizen focus groups, and their public oversight bodies. We see also that some LEAs have created ethics boards to advise on their use of advanced technologies,[117] and can recommend that LEAs consider creating such oversight structures if their current structures do not provide a similar level of expertise and oversight.

> *Recommendation for LEAs to engage stakeholders on the procurement and use of ROXANNE, and consider implementation of an ethics board.*

[112] Rosenberg, Nathan, Inside the Black Box, Cambridge University Press, Cambridge, 1983, p.48.
[113] Foucault, 1995, p.209.
[114] Foucault, 1995, p.213-214.
[115] Foucault, 1995, p.222-223.
[116] Foucault, 1995, p.207.
[117] See, for example, West Midlands Police and Crime Commissioner, "Ethics Committee". Available at: https://www.westmidlands-pcc.gov.uk/ethics-committee/ .

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

Resource re-use

Excessive and wasteful use of energy would seem to violate principles of environmental wellbeing. It would be ideal to avoid this, or to re-purpose some of the energy wastage. For example, if ROXANNE is used in a data-centre, or large data-processing facility, it might be possible to use water-cooling for these installations and repurpose the heated water for other uses.[118] This would seem to not only provide a use for what would otherwise be wasted heat and energy, but could also provide an additional income for the users of ROXANNE.

> *Requirement for technical partners to consider reducing the amount of energy used by ROXANNE, not yet possible to evaluate.*
>
> *Recommendation for partners to consider if wasted energy could be re-used, not yet possible to evaluate.*

Accountability

Any subsequent use of the operational ROXANNE platform by end-users holds them accountable for the tool's use in accordance with applicable national legislation and/or organisational code of ethics. However, the technology integrated oversight and access control mechanisms should help ensure compliance and deter potential abuses by authorised system users, which can be detected through logs verification (i.e. purpose of search, user details,). This logging system allows management to monitor the platform and ensure that it is used in a compliant manner. Additionally, training users on good practices prior to their first interaction with the ROXANNE technology is recommend for a sound understanding of the platform's functioning, accurate interpretation of results, and to remind users of associated ethical considerations.

> *Requirement for the ROXANNE platform to have integrated oversight mechanisms and access controls, not yet possible to evaluate.*
>
> *Requirement for the training provision to incorporate good practice regarding the ethical responsibilities of end-users, not yet possible to evaluate.*

[118] Jones, Nicola, "How to stop data centres from gobbling up the world's electricity" Nature, 2018. Available at: https://www.nature.com/articles/d41586-018-06610-y

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

3. T3.2: Comply with societal values

The task description of T3.2 provides the following:

> *'CAP and TRI will conduct a literature review on societal values and draft a workshop briefing paper. A workshop with external AB members will be convened (i.e. end-user workshop organized at KEMEA in M9) to discuss (a) how the project will address societal values and (b) what measures can be taken to avoid any harm to societal values. The partners will create a series of brief scenarios (vignettes) featuring different societal values (as the perception of security, possible side effects of technological solutions and societal resilience) and how the project will address them, post them on the project website and invite reactions from citizens.'.*

CAP and TRI conducted a literature review of academic journal articles and books, industry reports and news articles. Both began by searching online for resources about societal values, and how they relate to the ROXANNE project and platform. CAP and TRI used a 'snowballing' technique to follow references from this literature in order to find more resources. Over 60 items of immediate relevance were found and were used to write the briefing paper included below. Documents that were not found to be of specific relevance to either the ROXANNE platform or project were discarded. This literature review led to a list of societal values that CAP and TRI agreed were most pertinent to ROXANNE. [119]

CAP and TRI analysed each value in three stages: first, describing the value in terms of how it can relate to ROXANNE; second, potential issues that the ROXANNE project or platform could pose to these values; third, potential mitigation measures to deal with these issues. This led to development of the briefing paper below. In addition, to further gain insight into how ROXANNE could affect societal values, the scenarios below have been developed to expose potential issues that could arise. These have been discussed with LEAs in the project to check their realism, and, although there are differences across LEA practices, feedback suggested that they were realistic.

The intention in the Grant Agreement was to distribute the briefing paper and scenarios to persons who would attend the first field-test and discuss the topic of societal values in ROXANNE with these people to gather feedback on the efficacy of feasibility of the proposed solutions that are suggested in the briefing paper. The advantage of a briefing paper is that is provides a relatively concise and digestible summary of the issues at play for a non-specialist audience. It can act as a stimulus for discussion. The benefit of using scenarios is that they can situate abstract issues into a position that is more relatable for persons who are non-experts in societal values, and so can enable them to participate in discussion and offer useful feedback.

As the first field-test was delayed due to the ongoing Coronavirus pandemic, the workshop was also delayed. During planning of the rearranged virtual field-test, it was determined that a shorter event would be best for external attendees and so the workshop on societal values should take place separately later.

We will be conducting a webinar based on this deliverable and will talk about the ethical aspects, societal values, and legal aspects of ROXANNE. We intend to conduct this webinar around the end November 2020. The invited audience will include the External Ethics Board, Stakeholder Board, the consortium partners and other stakeholders from project's contact list.

In order to gather feedback on the briefing paper and scenarios, CAP and TRI will post both the briefing paper and scenarios online and will use the EU survey platform for attendees to the webinar, and citizens online, to provide feedback both on the proposed solutions, and the scenarios. The intention for T3.2 was to include the feedback and any updates to the briefing paper in this deliverable. However, owing to the delays, any alterations to the solutions will be noted in D3.4 (Final report on compliance with ethical principles).

[119] CAP analysed the following societal values: citizens' privacy; trust and the perception of safety; unintended consequences of technological solutions; social acceptability. TRI analysed: democracy and solidarity; equality and tolerance for other cultures; human rights; respect for human life the rule of law.

3.1. Briefing paper

This document includes requirements coming from the societal values analysis, in order to display them with those from the ethical and legal analysis. They will be removed from the briefing paper before it is disseminated.

Introduction

ROXANNE (Real time network, text, and speaker analytics for combating organized crime) is an EU funded project, aiming to enhance the identification of suspected criminals and their networks in investigations of organised crime and terrorism. It aims to do this by developing novel speech, text, and video analysis technologies to speed up the process of identification and fusing these outputs with network analysis in order to improve the visualisation of how criminal groups communicate. These will be brought together into the ROXANNE platform.

There are ethical and legal issues raised when producing surveillance technologies. The ROXANNE project will include principles of privacy-by-design and ethics-by-design. Key parts of these processes are considering the impacts this technology could have on a societal level. This briefing paper outlines values that are important in European societies. Societal values are '*principles or moral standards held by a person or social group'* and are '*generally accepted or personally held judgement of what is valuable and important in life'*.[120] They are used in this paper to display the potential impacts that the use of the ROXANNE platform could have on society, and how these effects can be mitigated. Also included are scenarios that highlight potential issues in future uses of the platform; we welcome comments and suggestion on these scenarios.

Societal Values

Citizens' privacy:

Privacy means '*the right* [for people] *to keep their personal life or personal information secret or known only to a small group of people*'.[121] This value is closely associated with the value of individual freedom which is defined as '*the condition or right of being able or allowed to do, say, think, etc. whatever you want to, without being controlled or limited*'.[122] This value is critical in the sense that citizens need to believe that no aspect of this project will hamper their rights. Privacy can be impacted when technologies are not used as intended; when their intended use impacts inappropriately upon privacy, or when they are inadequately secured allowing others to inappropriately exploit them.

A fundamental issue with platforms that process biometric data is data-subject privacy and trust in the platform.[123] There is a possibility of the platform being used for unintended purposes which might differ from what was initially envisioned. This is called 'function creep',[124] an obvious example would be a platform

[120] See 'Value' 6d, Oxford English Dictionary, OUP, UK, 3rd edn. 2011.

[121] See 'Privacy' B2, Cambridge Advanced Learner's Dictionary & Thesaurus, CUP, UK. Available at: https://dictionary.cambridge.org/dictionary/english/privacy

[122] See 'Freedom' B2, Cambridge Advanced Learner's Dictionary & Thesaurus, CUP, UK. Available at: https://dictionary.cambridge.org/dictionary/english/freedom

[123] Ashbourn, Julian, "Background paper for the Institute of Prospective Technological Studies", European Commission DG Joint Research Centre, 2005. Available at: http://www.statewatch.org/news/2005/apr/jrc-biometrics-julian-ashbourn.pdf

[124] Dekkers, Dick, "Privacy or security? - 'Function Creep' kills your privacy", Digidentity, 2016. Available at: https://www.digidentity.eu/en/article/Function-creep-kills-your-privacy/

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

intended for targeted surveillance being used for mass surveillance.[125] "Chilling effects" occur when such platforms might impede citizens' freedom to act due to the fears of misappropriation of biometric data or of a totalitarian future.[126] One of the possible repercussions of such a scenario could include attempts to control the public behaviour by leveraging the fear of being monitored.[127] This shows how intrusions into public privacy can lead to serious consequences.

As part of including privacy and ethical concerns into the design process of the ROXANNE platform, technical partners in the project should first ensure a sound legal basis for processing of personal data, with a clear link between the design of the platform and the necessity for processing such data. This should be based upon scientifically valid causal models (e.g, we have good scientific reasons to believe that processing a particular form of personal data will lead to useful and effective analytic tools). From a security perspective, they should ensure that the data is completely secured from any unauthorised access by implementing efficient data protection measures. They should further incorporate data-security in the system architecture by design and by default.[128] This includes measures such as conducting data protection impact assessments, writing apt privacy policies in easy-to-understand language, providing data-subjects information on how their data is used and who they can contact about it, ensuring that personal data is not automatically made publicly available to others etc.[129]

Requirement for technical partners to only process personal data according to a sound legal basis, completed so far in the project.

Requirement for there to be a clear link between the need to process particular data and the design of the platform, completed so far in the project.

Requirement for the technical partners to incorporate data security by design and by default in the system architecture while ensuring lawful data processing, completed so far in the project.

Requirement for ROXANNE partners to conduct data protection impact assessments where required, write easy-to-understand privacy policies, provide information about processing to data-subjects, and not make personal data automatically available to the public, completed in the project so far where required.

Further, ensuring that data processing in the ROXANNE platform follows data protection legislation applicable to law enforcement activities[130] would be the key to preventing unauthorized data sharing. With respect to collection of data during operational use, the onus of using lawfully collected data would be on the end-user of the platform. The platform should support use-logging and access control to allow its use to be appropriately audited. However, the consortium must be very careful with respect to the organisations' who would be given access to this platform by conducting due diligence to make sure that the platform will not be abused by the end-users and would only be used for law enforcement. End-users will only be responsible law enforcement agencies (LEAs), mostly likely in Europe. All these measures should help mitigate the concerns related to citizens' privacy.

Recommendation for LEAs to follow data protection legislation in any use of ROXANNE.

Recommendation for LEAs to ensure data processed using ROXANNE was lawfully collected.

[125] Pastukhov, Oleksandr and Els Kindt, "Voice Recognition: Risks to Our Privacy", Forbes, 2016. Available at: https://www.forbes.com/sites/realspin/2016/10/06/voice-recognition-every-single-day-every-word-you-say/#2621e79e786d

[126] Zuboff, Shoshana, "The Surveillance Threat Is Not What Orwell Imagined", Time.com, 2019. Available at: https://time.com/5602363/george-orwell-1984-anniversary-surveillance-capitalism

[127] Ievdokymova, Iryna, "Surveillance and profiling: what's next?", Leidenlawblog, 2013. Available at: https://leidenlawblog.nl/articles/surveillance-and-profiling-whats-next

[128] Art.25, GDPR.

[129] Irwin, Luke, "What is data protection by design and default?", Itgovernance, 2019. Available at: https://www.itgovernance.co.uk/blog/what-is-data-protection-by-design-and-default

[130] Art.1(1), LED.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

> *Requirement for technical partners to facilitate LEAs attesting to lawful data collection, not yet completed.*
>
> *Requirement for exploitation to be limited to responsible LEAs who maintain a good track-record of complying with human rights, not yet possible to evaluate.*

Trust and the perception of safety:

People have trust in others when they '*believe that someone is good and honest and will not harm you, or that something is safe and reliable*'[131]. It is imperative for citizens to feel confident with respect to deployment of the ROXANNE platform, and that it will make them feel safer in their societies. This confidence will be closely correlated to the trust that citizens have in the organisations involved in using the ROXANNE platform.

Uses of the ROXANNE platform could misuse personal data in ways that abuse the trust of citizens. One possibility could be using the platform to run network analysis on individuals who are not directly associated with any known suspects. This would increase apprehensions of mass-surveillance and abuse of power by the state. Also, any bias in processing of data based solely on the difference in creed, colour, race or religion, which would be tantamount to discrimination by design, could increase distrust with respect to the platform. Algorithmic transparency is a crucial step to further the cause of garnering trust in the platform;[132] project partners should be able to explain how the platform works in order to give citizens an idea of how they can expect any data LEAs collect on them to be processed.

> *Requirement for technical partners to build the ROXANNE platform in such a way that it can be understood, and its processes and decisions can be explained to the public, not yet completed.*

A lack of faith in LEAs deploying this platform, might also lead to suspicion over the intended or actual use of this platform. To mitigate these concerns, end-users (LEAs) should play an active role in trust-building actions regarding this platform.[133] In order to inform citizens and increase their trust in the platform, end-users should, as far as possible, provide information about how use of surveillance platforms is overseen and discuss with local populations; this should increase the security of society as a whole whilst reducing the scope for the abuse of power by end-users.[134] LEAs should also be open about data retention timespans (or criteria for determining whether to store personal data), and how data-subjects can be exercise their rights, along with training individuals to ensure ethical conduct while processing data. Moreover, every activity on the ROXANNE platform should be logged so that it can be audited. It should also be clear to citizens how end-users can be held accountable for cases of misusing surveillance platforms.

> *Recommendation for LEAs to be open with the public about their data-protection policies, including data-retention and how data-subjects can exercise their rights.*
>
> *Requirement for technical partners to built the platform in such a ways to enable logging of data-processing activities, not yet completed.*

A recent whitepaper by the European Commission has suggested a comprehensive approach to build trust in AI systems through developing an 'ecosystem' of trust where all applicable laws are complied with and multiple entities have oversight of such systems.[135] End-users should consider implementing internal oversight

[131] See 'Trust' B1, Cambridge Advanced Learner's Dictionary & Thesaurus, CUP, UK. Available at: https://dictionary.cambridge.org/dictionary/english/trust

[132] Epic, "Algorithmic Transparency: End Secret Profiling", Epic. Available at: https://epic.org/algorithmic-transparency/

[133] Swaminathan, Aravind and Antony P. Kim, "Biometrics: A Fingerprint for Privacy Compliance, Part I", Orrick, 2016. Available at: https://blogs.orrick.com/trustanchor/2016/03/04/biometrics-a-fingerprint-for-privacy-compliance-part-i/

[134] European Parliament, "A governance framework for algorithmic accountability and transparency", EU, 2019. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624262/EPRS_STU(2019)624262_EN.pdf

[135] European Commission, "Whitepaper on Artificial Intelligence - A European approach to excellence and trust", EU, 2020, pp.9-10. Available at: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

measures to monitor deployment of such systems, but also external measures to evaluate processes for using the platform and its outputs, a key indicator for this having large scale pilots/trials.[136] Examples of such oversight include the West Midlands Police (UK) ethics board which has included lay members of the public and has been active in consideration of the development of predictive policing tools.[137]

> *Recommendation that LEAs consider implementing internal oversight mechanisms to evaluate use of data-processing technologies for operations.*

Unintended consequences of technological solutions:

Technologies are generally adopted for the benefits that they bring. However, there are often additional features of technologies that create consequences for their users and the public that are not beneficial. Understanding the implications of using a technology and the effects they can create is important for society as it helps all stakeholders get a better understanding of undesirable technical features of different platforms.There are also systems where benefits for end-users have negative (externalised) consequences for other groups, a problem that particularly affects marginalised and vulnerable populations, whose needs and circumstances are not taken into account in the design and deployment of a technology.[138] Externalised consequences can include impacts on other social values.

Biometrics based systems have some inherent limitations.[139] For instance, in voice/speech based biometric systems, a suspect's sample might actually sound different depending on person's health, time of the day and even depending on who the person is interacting with;[140] they could also be mimicked and fool a recognition algorithm.[141] Another example could be that of probabilistic outcomes, such as false-positives (highlighting an innocent citizen) or false-negatives (not recognizing a potential suspect),[142] which could cause issues for those individuals and the public. Further, if the end-users are not well trained, they might use the platform in a mistaken manner to get fallacious results.[143]

To tackle these issues in ROXANNE, technical partners should ensure that recognition technologies are accurate enough to identify targeted persons, but also have some variance to account for different circumstances that might affect the quality of data collected during operations. These technologies should also

[136] Institute for Prospective Technological Studies, "Biometrics at the Frontiers: Assessing the Impact on Society", European Commission DG Joint Research Centre, 2005. Available at: http://www.statewatch.org/news/2005/mar/Report-IPTS-Biometrics-for-LIBE.pdf

[137] Heubl, Ben, "West Midlands Police strive to get offender prediction system ready for implementation, E&T, the IET, September 24, 2019. https://eandt.theiet.org/content/articles/2019/09/ai-offender-prediction-system-at-west-midlands-police-examined/

[138] Noble, Safiya, Algorithims of Oppression, NYU Press, New York, 2018; Eubanks, Virginia, Automating Inequality, St Martins Press, New York, 2018, and Benjamin, Ruha, Race Against Technology, Polity Press, 2019

[139] Prabhakar, Salil, Sharath Pankanti, and Anil K. Jain, "Biometric recognition: security and privacy concerns", *IEEE Security & Privacy*, Vol.1, No.2, March-April 2003, 33-42.

[140] Scheips, Derek, "Voice Recognition – Benefits And Challenges Of This Biometric Application For Access Control", Securityinformed. Available at: https://www.securityinformed.com/insights/co-3108-ga.4100.html ; Ahaskar, Abhijit, "Voice biometrics are cleverer now, but still need more work", Livemint, 2020. Available at: https://www.livemint.com/technology/tech-news/voice-biometrics-are-cleverer-now-but-still-need-more-work-11581011267941.html

[141] Panjwani, Saurabh and Achintya Prakash, "Crowdsourcing Attacks on Biometric Systems", USENIX, 2014. Available at: https://www.usenix.org/system/files/conference/soups2014/soups14-paper-panjwani.pdf

[142] Penny, Wayne, "Biometrics: A Double Edged Sword - Security and Privacy", SANS Institute, 2020. Available at: https://www.sans.org/reading-room/whitepapers/authentication/biometrics-double-edged-sword-security-privacy-137

[143] Zadelhoff, Marc van, "The Biggest Cybersecurity Threats Are Inside Your Company", Harvard Business Review, 2016. Available at: https://hbr.org/2016/09/the-biggest-cybersecurity-threats-are-inside-your-company ; SSE, "KnowBe4 Benchmarking Report: Untrained Users Pose The Greatest Risk To Your Organization", SSE. Available at: https://www.sseinc.com/cyber-security/knowbe4-benchmarking-report-untrained-users-pose-the-greatest-risk-to-your-organization/

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

be thoroughly tested to ensure that the incidence of false-negatives and false-positives is not so great as to cause difficulties for impacted populations. As these issues can only be mitigated and not resolved, it is important that information about them is included in the training provision to be given to end-users so that they can understand the limitations of the platform and the implications of using it.

> *Requirement for technical partners to optimise the accuracy of algorithmic outputs, whilst taking risks of false positives and false negatives into account, not yet possible to evaluate.*

> *Requirement for training provision to include information on the limitations of the platform, and implications of use, not yet possible to evaluate.*

Social acceptability:

Acceptability can be described as '*the quality of being satisfactory and able to be agreed to or approved of* '.[144] Project partners are trying to develop the ROXANNE platform in a way that citizens trust it after appreciating the pros and cons associated with the platform. As public servants, LEAs need to use tools/technologies that are socially acceptable.

The willingness to accept key aspects of innovation among all stakeholders can be subdivided into two broad segments: (a) acceptance of the creation of the socio-economic conditions needed for implementation and (b) acceptance of all consequences of the innovation. The latter refers to the ways in which implementation will affect and change current practices in society.[145] Further, social acceptability is a result of citizens' attitude towards the overall proposition (use of the ROXANNE platform in this case). This attitude could be influenced by awareness about perceived risk/uncertainty, values or beliefs of the citizens, trust in the users and developers of the platform, participation in decision making process, potential benefits from the project etc.[146]

Literature on the technology industry suggests that citizens are overwhelmingly more likely to trust organisations with strong privacy policies, and those who are transparent about how they use data.[147] Assuming that people view public and private organisations in similar ways when it comes to trusting that they use data in compliance with ethical and legal standards, then this indicates that having LEAs be open about their data processing and a strong privacy policy should enhance citizen's trust of LEAs.

> *Recommendation for LEAs to be open about the types of data-processing operations they engage in using ROXANNE.*

> *Recommendation for LEAs to have strong privacy policies that are publicly available.*

Indeed, citizens are unlikely to find biometrics based platform such as ROXANNE acceptable where: they fear it could be used for mass surveillance, or to encroach upon their privacy; when they do not trust the police;[148] or when they are uncomfortable with an organisation holding sensitive data about them.[149] Thus, providing citizens a complete picture of the platform, its policies and fairness of process becomes imperative. For citizens to be able to trust that LEAs use their data properly, LEAs need to be able to demonstrate that the use of

[144] See 'Acceptability', Cambridge Advanced Learner's Dictionary & Thesaurus, CUP, UK.
Available at: https://dictionary.cambridge.org/dictionary/english/acceptability

[145] Wolsink, Maarten, "The research agenda on social acceptance of distributed generation in smart grids: Renewable as common pool resources", Elsevier, Vol.16, Issue 1, January 2012, 822-835.

[146] Government of Quebec, "Social Acceptability", Quebec.ca, 2019. Available at: https://www.quebec.ca/en/government/policies-orientations/social-acceptability/

[147] Fraser, Adam, "Is an ethical approach to customer data privacy your trust differentiator?", EY, 2020. Available at: https://assets.ey.com/content/dam/ey-sites/ey-com/en_au/topics/data-privacy/ey-is-an-ethical-approach-to-customer-data-privacy-your-trust-differentiator.pdf

[148] Goldsmith, Andrew, "Police reform and the problem of trust", Sage Publications, London, 2005. Available at: http://www.slcdocs.com/ODHR/Website/Right%20to%20Safety/Literature/PoliceReformAndTheProblemOfTrust.pdf

[149] Ada Lovelace Institute, "Beyond face value: public attitudes to facial recognition technology", Ada Lovelace Institute, 2019. Available at: https://www.adalovelaceinstitute.org/wp-content/uploads/2019/09/Public-attitudes-to-facial-recognition-technology_v.FINAL_.pdf

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

ROXANNE would in no way affect the security or freedoms of innocent people. Steps toward this can include raising awareness about the accuracy and data security of the platform and taking citizens feedback into account wherever possible.

> *Requirement for technical partners to include information on accuracy and data-security in dissemination activities, not yet possible to evaluate.*

Citizens are usually only indirectly involved in the development of novel technologies. They shape the innovation process by voicing their opinions or by displaying actions that support or resist a technology, both after and before market introduction. However, the overall public acceptance for a such a technology can be gauged through opinion polls that represent aggregated attitude of citizens.[150] This feedback is key to making citizens part of the decision-making process and raising their confidence in this platform. This input will help guide the design, dissemination as well as exploitation of this platform as a whole, which in turn encourage greater social acceptability.

> *Requirement for technical partners to take citizens' feedback into account during platform development, not yet possible to evaluate.*

Further, by engaging in a continuous effort towards creating a platform which is built keeping in mind all other societal values, we can increase the probability of social acceptability for this project. This includes raising awareness about the platform as a whole. The consortium should inform the citizens about the extent of data security to make citizens feel safe about their data. The consortium should also highlight the extent to which this platform will help prevent crime while ensuring swift identification of suspected criminals. However, it is equally significant to inform citizens about the possibility of false-positives and false negatives and how the project is dealing with this; oversight mechanisms, and the process set forth to rectify errors in such a situation. The consortium should also spread awareness about legal measures that protect citizens from unjust effects of processing of their personal data.

> *Requirement for ROXANNE partners to highlight data-security measures, the expected impact ROXANNE will have on preventing and fighting crime, how the project is dealing with risks of false negatives and false positives, oversight mechanisms, and legal protections, not yet possible to evaluate.*

Democracy and solidarity

Democracy is a popular method of collective decision-making, particularly in political systems. Key to the implementation of democracy is that the people who participate in the decision-making are treated equally and have the necessary liberties to engage in it.[151] This is an important societal value as it allows people to group together in solidarity with others to pool their collective power for common causes (for example, political movements).

There is potential for the ROXANNE platform to affect democratic expression. For example, a person is less likely attend a political rally if they believe that they will be subject to surveillance by state agents and this will lead to unfavourable treatment by the state; this is an example of a 'chilling effect'.[152] ROXANNE poses a particular issue if its users identify people under surveillance and then use its network analysis capabilities to identify other people in the networks of political activists. This increases the likelihood of such chilling effects as people will be further disinclined to partake in particular activities so as not to implicate their friends and family. If this effect is realised, it is likely to lead to less political participation from the public and an acceptance of the *status quo* to protect their acquaintances, despite not being in favour of it.

[150] Rijnsoever, Frank J. van, Allard van Mossel and Kevin P.F. Broecks "Public acceptance of energy technologies: The effects of labeling, time, and heterogeneity in a discrete choice experiment", Elsevier, Vol.45, May 2015, 817-829.

[151] Christiano, Tom, "Democracy", The Stanford Encyclopaedia of Philosophy, 2006. Available at: https://plato.stanford.edu/entries/democracy/

[152] Solove, 2006, 477-560, 487.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

These risks can be mitigated through preventing sales of the ROXANNE platform to authoritarian states, or actors who might engage in repression of persons who attend political events. Further, the implementation of decision-making processes that require ethical and legal compliance in order for the platform to function should prevent the platform being abused where these processes are followed. The legitimate use of ROXANNE is somewhat dependent on proper training of the end-users, and the incorporation of end-user training as part of the ROXANNE project should contribute to this.

> *Requirement for ROXANNE partners to avoid exploitation to authoritarian states, not yet possible to evaluate.*
>
> *Requirement for ROXANNE partners to implement processes to ensure decision-making processes prevent use of the platform in contravention with ethical and legal standards, not yet possible to evaluate.*
>
> *Requirement for training provision to highlight ethical and legal issues, not yet possible to evaluate.*

Equality and tolerance for other cultures

Equality is a societal value that holds all people to be equal whatever their differences. This is an important value as it enables all people to be treated fairly,[153] no matter what their status. This is a key principle of International and European political and legal systems.[154]

ROXANNE has the potential to affect people from different social groups in a disproportionate way. Bias in the outputs of a platform can be caused where: a data set used to train the models is biased toward or against a particular group; the dataset is not representative of the environment it will be used in, or the population it will be used with; where the system is not measuring representative data.[155]

For example, members of a group might be treated differently by a facial recognition algorithm due to the colour of their skin where the model has been trained on more pictures of people from one ethnic group than another.[156] This is an issue of particular relevance to policing. Where existing police data is biased and provides a skewed view of a particular group, then that affects how the outputs of data-analysis systems are assessed. If this influences future policing, it can lead to a compounding of bias.[157] However, it is complicated further by factors specific to criminality such as the greater prevalence of more crimes being committed by young men in comparison to other groups.[158] The impact of producing a system to specifically targeted these people is that biases are reproduced and such persons are at significant risk of being discriminated against.

The ROXANNE consortium should do all that it can to alleviate risks of this happening through evaluating all the data sets which it is using to train the platform on to ensure that they are not biased for or against different

[153] See, for example, Rawls, John, *Justice as Fairness: A Restatement*, Belknap Press, United States, 2001.
[154] See, for example, International Convention on the Elimination of All Forms of Racial Discrimination (adopted 7 March 1966, entered into force 4 January 1969) 660 UNTS 1; Directive 2006/54/EC of the European Parliament and of the Council of 5 July 2006 on the implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation (recast) OJ L 204, 26.7.2006.
[155] Woodie, Alex, *Three Ways Biased Data Can Ruin Your ML Models*, datanami, 2018. Available at: https://www.datanami.com/2018/07/18/three-ways-biased-data-can-ruin-your-ml-models/
[156] See, for example, EU Agency for Fundamental Rights*, #BigData: Discrimination in data-supported decision making*, FRA, 2018.
[157] Babuta, Alexander and Marion Oswald, *Data Analytics and Algorithmic Bias in Policing*, RUSI, 2019, pp.11-12. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/831750/RUSI_Report_-_Algorithms_and_Bias_in_Policing.pdf
[158] See, for example, Schwartz, Jennifer, et al. "Trends in the Gender Gap in Violence: Reevaluating NCVS and Other Evidence" *Criminology*, Vol.47, No.2, May 2009, pp.401-425; Devon, James, "Age and Crime" *The Police Journal*, Vol.65, No.3, July 1992, pp,268-273.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

groups, and ensuring that the platform is measuring data that is representative. This should, therefore, reduce the risk of the ROXANNE platform having a discriminatory effect when it is used.

> *Requirement for technical partners to implement measures to assess and minimise the effects of biased data on ROXANNE tools, or incorporate diversity into training datasets, not yet possible to evaluate.*

Human rights

Human rights are legal rules that require states to respect and protect people. They also provide a framework where state actors can infringe upon rights in situations where this is necessary and proportionate. Privacy rights are well known, and these can be lawfully infringed upon in some situations such as where law enforcement needs to know private information in order to prevent or investigate serious crimes.[159]

There is always a risk with data-analysis technologies that they could be used in a way that is arbitrary, meaning that it is not necessary or proportionate to use in a specific situation. However, ROXANNE poses particular risks as it analyses not only at the individual who police are interested in but also at whom they communicate with; it could be arbitrary to include their associates in the surveillance activities.

In order to mitigate this risk, the ROXANNE platform should only be sold to law enforcement agencies in states with a good human rights record. The platform could be built to include decision-making process that require law enforcement officers to take a decision on whether to include or exclude the data of associates from a network analysis, the decision-making processes will incorporate the human rights legal framework in order to facilitate compliance.

> *Requirement for decision-making processes to enable compliance with human rights law by requiring end-users to explain the necessity and proportionality of their data-analysis activities, not yet possible to evaluate.*

Respect for human life

Recognising that all people have an inherent dignity is a societal value that underpins human rights, equality, and fair treatment of others.[160] Where people ignore the dignity of others, this is a process of dehumanisation and people are treated as less than human, resulting in systematic atrocities at its worst extent.[161] Data processing about people can lead to a less dramatic form of dehumanisation where people are treated as mere data points, leading people to forget that the outputs of algorithmic systems have real consequences for other human lives.

With ROXANNE, this could be particularly problematic where, for example, the platform is used to analyse police surveillance data and operational decisions are made based on the outputs of the platform, rather than a police officer evaluating the person under investigation. Or an investigator trusts an algorithm, rather than making the decision themselves. For example, this could lead to a citizen being subject to further investigation and analysis of their sensitive data even though their actions are perfectly innocent, and this would have been understood had a human evaluated the original results in a meaningful way.

These risks can be mitigated in the ROXANNE platform through structuring the relationship between human and machine to avoid (or minimise) issues of blindly following machine outputs (automation bias), and to prioritise human decision-making. Technical partners should structure the human-machine relationship so that the benefits of machine analysis are used to complement human decision-making.

[159] See, for example, Article 8, European Convention for the Protection of Human Rights and Fundamental Freedoms (adopted 4 November 1950, entered into force 3 September 1953) 213 UNTS 221.

[160] See, for example, Preamble, Universal Declaration of Human Rights (3rd session, 10 December 1948) UN Doc. A/RES/217(III).

[161] Smith, David L, "Dehumanization, Essentialism, and Moral Psychology", *Philosophy Compass*, Vol.9, Issue 11, 2014, 814-824.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

Requirement for ROXANNE partners to build the platform in such a way as to avoid automation bias and prioritise human decision-making, not yet possible to evaluate.

Recommendation for LEAs to use ROXANNE as an assistive tool in human-led investigations.

The rule of law

Having all people and institutions subject to legal rules and legal frameworks is a key aspect of democratic systems as it prevents different parts of the system from gaining excessive power. This is a key societal value as it allows people to trust their institutions.[162]

ROXANNE does not necessarily pose a direct risk to this system or trust in institutions. But, human beings often give greater weight to the outputs of advanced technologies over themselves or other human beings.[163] In the context of a criminal trial, this could pose an issue whereby evidence from the surveillance data analysed by the ROXANNE platform is given greater weight than evidence from other surveillance technologies would normally be given. This could, potentially, mean that the results of data analysis are seen as more conclusive than they should be, and this could lead to misunderstandings in court. Potentially, this could affect how the guilt or innocence of a defendant is viewed in court.

A way to mitigate this would be for ethical/legal partners to disseminate information about this risk to highlight this issues so that it can be properly understand that whilst ROXANNE and similar technologies are advanced, this should not mean that evidence generated from them should be given significant weight in a criminal trial. Potential recipients could include groups representing judges and lawyers.

Requirement for ethical/legal partners to disseminate information about risks of advanced technologies for court proceedings, not yet possible to evaluate.

Emerging themes

This paper discusses the issues that could be raised from the potential use of the ROXANNE platform in terms of societal values. Some values place importance on independent oversight of LEAs using the ROXANNE platform with accountability measures to increase compliance with applicable standards. These are important features about the organisations that will use ROXANNE. In terms of the platform itself, ensuring transparent processing and un-biased algorithms are important as this should result in fair treatment of citizens by the platform, and an ability for LEA officers to understand what is happening inside the platform to enable them to make fully informed decisions for their investigations. Another important theme is that LEAs should only use the ROXANNE platform in a way that is lawful and appropriate for the investigation at hand. These themes, amongst other issues, show that whilst violations of privacy are undesirable for society, they can be carried out in conformity with societal values where they are fair, lawful, and subject to accountability measures. In the specific case of using ROXANNE, ensuring that a human being is in control of deciding how to use machine outputs also seems to be a key requirement for compliance with societal values.

These societal requirements may appear to misalign with the project objective of increasing the speed at which organised crime investigations can take place: increasing the human role and oversight can slow down uses of automated systems. Yet, this need not be an issue for the use of ROXANNE as the overall speed of an investigation, even with the necessary human input, might well progress faster than the current tempo of investigations. Further, when the appropriate permissions and authorisations are in place, the investigation time will reduce. As such, human oversight both of the platform and the process of using the platform should not be sacrificed simply to increase the speed of investigations.

[162] Postema, Gary J, "Trust, Distrust, and the Rule of Law", in Paul B. Miller and Matthew Harding (eds.), *Fiduciaries and Trust: Ethics, Politics, Economics and Law*, CUP, Cambridge, Forthcoming. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3394978

[163] See, for example, Skitka, L.J., Kathleen L. Mosier and Mark Burdick, "Does Automation Bias Decision-Making?" *International Journal of Human-Computer Studies,* Vol.51, 1999, 991.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

3.2. Scenarios

Scenario 1 – suspected child abuse

An LEA (A) of a European nation receives intelligence from an LEA (B) in a neighbouring country regarding a possible perpetrator of child exploitation. The LEA (B) has used the ROXANNE platform to recognize voices in phone calls which match to those recorded in previous investigations from 2019. One of the calls is traced to Mark's house. His house falls under the jurisdiction of LEA (A). Mark lives with his wife, two children, and his father in a sophisticated area of the city. According to the tip, several infrequent telephone calls have been made to known child abusers from the house owned by Mark. These child abusers are associated with uploading homemade content to a dark web site.

Question: Would you (LEA A) require any information about the use of a data-analysis platform by LEA (B) upon receipt of intelligence ? Would you need to know specific results of the data analysis? Would you want to know which analysis platform was used?

Answer:

The LEA (A) investigates Mark and discovers he has sometimes travelled to locations near to known child abusers who have called his house. Using intelligence about metadata of phone calls from the LEA (B), investigators use ROXANNE to visualise a network of communications between child abusers, with Mark's phone shown to be prominent in the network.

LEA (A) officers request to place Mark under surveillance. After considering multiple documents, including the results of the ROXANNE platform, a judge gives the required permission for surveillance. This includes intercepting the voice calls from the landline phone in Mark's house, and footage from the CCTV cameras near Mark's house.

Question: Is it likely that a judge would authorize surveillance in your country based primarily off the results of a data-analysis platform? Would other corroborating evidence be required?

Answer:

After three days of surveillance, the speakers in a voice call from Mark's house are matched by the ROXANNE system. The caller speaks very little on the call, and the ROXANNE system suggest it is more likely than not that the caller is Mark. The LEA officers assume that the caller is Mark and the short voice samples are the reason that the match is not more definitive. The call recipient speaks a lot on the call and their voice is matched by the ROXANNE system to a known child abuser. The LEA (A) officers conclude from this that Mark is in direct contact with known child abusers.

On another call, Mark heard discussing a business trip to another city and the investigators are concerned that he might meet other child abusers. Officers begin to look into putting Mark under surveillance for the duration of his business trip.

Question: Could you foresee a situation where LEA officers make decisions just based off the results of a data-analysis platform, rather than also using their intuition and experience? Would this concern you?

Answer:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

In the days before Mark's business trip new video content is uploaded to the dark web site used by the child abusers. The video metadata shows that the video was recorded one day earlier. The face of one of Mark's children is recognised in the video content by the ROXANNE platform that is comparing the video with CCTV images.

Owing to the child protection risks, LEA (A) officers raid Marks house. Mark, his wife and father are arrested, and his children are taken into temporary care by the authorities.

Question: It is likely that you would incorporate two streams of evidence from an investigation (e.g. video files gathered from CCTV and the dark web) for analysis? Or, would you only compare evidence with data in a verified database, for example?

Answer:

During questioning, it is shown that Mark and his wife were shopping all day when the abuse content was filmed. Mark's father, Simon, was staying in Mark's house and is shown to have a very similar voice to Mark. Upon further investigation, it is determined that Simon made the calls to child abusers from Mark's house and filmed the abusive content.

LEA officers take voice samples from Simon's police interviews and analyse them using the ROXANNE platform. Simon's voice matches with several samples from previous voice recordings associated with child abuse where the speaker was unknown.

Question: Would you need special permissions to process (biometric) data gathered in one case for another investigation? If so, what permissions would you require?

Answer:

Scenario 2 – suspected drug dealing

Frank is a member of an ethnic minority and lives in a community that has recorded a high crime-rate for a long time. He is seen interacting with known leaders of criminal organisations who are under video surveillance by officers investigating gang violence. Surveillance images are analysed using the ROXANNE platform which suggests a high-probability that Frank is actually William, the former leader of a drug gang who left the area several years ago. LEA officers who remember William think that Frank looks similar to, but not exactly like, their memories of William. They put the difference down to the years that have passed and trust the algorithm.

Question: How should the ROXANNE platform present the results of components that can recognise an individual? Display the most probable match? List the 10 most probable matches? List all those with a probability match above a certain percentage? Something else?

Answer:

Question: Should LEA officers be allowed to 'trust the algorithm'? Should algorithmic solutions only be used to inform an LEA officer's judgement? Should investigators corroborate data-analysis results they want to use?

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

Answer:

The determination that *William* has returned to the area is included in intelligence reports to a new regional anti-drug squad who are investigating a large and well-organised drug gang. Owing to *William* being observed interacting with criminal leaders, and William's extensive criminal record, investigators show the information they have to a judge who is also convinced that Frank is *William* and obtain a warrant to place *William* under surveillance by monitoring his phone calls, text messages, and emails.

Question: How should information about the results of recognition technologies be reported within and by LEAs? Reporting who was recognised? Reporting the probability of recognition? Something else?

Answer:

Question: If multiple people are recognised with a high probability, should all these possible recognitions be included in reports?

Answer:

Officers record several phone calls where *William* is heard telling the leaders of drug gangs that they should '*work for him*'. Investigators use the ROXANNE platform to visualise the connections between people whose communications are monitored; this shows *William* as a key node in a network with known criminals. *William's* emails also reveal that he manages a community organisation campaigning for better political representation of ethnic minorities. Owing to the strength of communications with many criminals, investigators theorise that the community organisation could be a front for hiding a criminal network run by *William*. They decide to investigate the community organisation further.

Question: How should the context of data analysis be conveyed? Should suspects, known criminals, and innocent people all be highlighted in some way?

Answer:

In their expanded investigation, LEA officers use the ROXANNE platform to analyse the seemingly innocent communications *William* has with his staff at the community organisation. The text analysis part of the platform outputs that staff members regularly use slang terms for drugs typical of criminal organisations, and the voice recognition part of the platform recognises several staff members of staff who are from ethnic minorities as having criminal records in an LEA database.

Question: If data from innocent persons is captured by LEA surveillance, how should these people's privacy be protected during data-analysis? What safeguards should be implemented?

Answer:

Question: Should data analysis systems have access to historical LEA databases even if those databases contain data generated by discriminatory policing practices from the past? What safeguards should be implemented?

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

Answer:

From all of these data, investigators conclude that *William* is overseeing a major drug dealing operation with several local gangs working for him. LEA officers decide to raid the community organisation for evidence of drug dealing. They find no evidence, but determine that Frank is not William and was in contact with criminals in order to try and convince them to leave their criminal activities and '*work for him*' at the community project. They also discover that the prevalence of criminal records and use of slang typical of criminal organisations is due to the community organisation hiring ex-prisoners as an example of rehabilitation.

Question: Is it likely that arrests could be made based purely on the results of a data-analysis platform? Would corroborating evidence be required?

Answer:

Owing to the sensitive nature of the investigation, LEA officers are unable to explain their actions in detail. This results in a loss of trust between the community and LEAs. It also deters people from engaging in legitimate political activism as some locals feel the community organisation was targeted for its political activities. Owing to the complexity of the algorithms used, LEA officers are also unable to explain why the platform made the determinations that it did.

Question: Should LEAs be open with the public about what surveillance tools they are using? How open should they be? How should they explain surveillance and data-analysis tools to the public?

Answer:

Question: If possible, would you like to know why data analysis platforms produce the results that they do? How much detail would be beneficial?

Answer:

Additional questions to be asked following both scenarios

1. According to your direct experience or research, do you see any particular societal risk associated to the development and use of technologies in the present scenarios which should be addressed in the context of the ROXANNE project?
2. Thinking about the deployment of the ROXANNE platform, in what situations, and at what stage of the innovation process, do you think it is necessary to carefully discuss and assess with society if its use is proportionate and appropriate to the problem it is aimed at solving?
3. Do you think that the ROXANNE platform could meet resistance from LEA officers, due to problems or issues concerning its societal utility, societal acceptability, or for other reasons? (If answer is yes) Please specify what kind of resistances
4. Do you think that the introduction of the ROXANNE platform might meet particular social resistances from citizens? (If answer is yes) Please specify what kind of resistances

5. What might be, according to your experience, possible advantages for society of LEAs using the ROXANNE platform compared to other existing technologies available?
6. What are, according to your experience, the disadvantages for society if LEAs were to use the ROXANNE platform in criminal investigations? Why? How can the ROXANNE platform overcome those limitations, according to your experience?
7. What are, in your experience, the most important ethical, legal, cultural and social aspects affecting social acceptability of surveillance oriented technologies that should be considered to ensure the ROXANNE platform meets the needs, values and expectations of society and mitigate societal concerns?

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

4. T3.3: Comply with fundamental rights

The task description for T3.3 provides the following:

> '*The partners will prepare an analysis about what and how fundamental rights might be impacted by the project's proposed solutions. The partners' analysis will be based on selected rights from the Charter of Fundamental Rights of EU. The analysis will provide several examples, like the vignettes in the previous task. The partners will disseminate the analysis to LEAs exploiting INTERPOL's global LEA network, policymakers, and civil society organizations*.'

In order to carry out this task, TRI conducted scoping work to determine which articles from the EU Charter of Fundamental Rights (EUCFR) were most relevant. The scoping work consisted of making an assessment of the *prima facie* relevance of each right to ROXANNE. This was used to narrow down the selected rights that are of most relevance to ROXANNE; for example, an analysis of the right to life is not included as ROXANNE does not in any way contribute to the use of lethal force by LEAs, and so that right is not particularly relevant to the project.[164]

The applicability of the EUCFR is limited, as stated in Article 51(1):

> '*The provisions of this Charter are addressed to the institutions and bodies of the Union with due regard for the principle of subsidiarity and to the Member States only when they are implementing Union law. They shall therefore respect the rights, observe the principles and promote the application thereof in accordance with their respective powers.*'

It is expected that, if made available for sale, the ROXANNE platform is expected to be used by LEAs enforcing their domestic criminal laws. This might involve implementing Union law to some degree (e.g. compliance with the Law Enforcement Directive).[165] However, as Union law is not implemented to the same extent as domestic law, and so does not have the same broad application as other human rights conventions, the partners in WP3 decided to broaden their enquiry with a comparative approach. Thus, where rights in the EUCFR and other human rights treaties are similar enough to provide greater insight, they are used to enhance understanding of the rights in the EUCFR.

This is somewhat already part of the approach taken by the EUCFR itself. In order to avoid development of competing human rights regimes dealing with the same issues, Article 52(3) of EUCFR provides:

> '*In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection*.'

Consequently, much of the discussion below refers to the articles of the European Convention, and the case law of the European Court of Human Rights, particularly in relation to specific rights that are read in the Charter as having the same meaning and scope as those in the Convention.

Further, in order that issues raised at the project stage are not ignored, the following analysis also incorporates a 'Business and Human Rights' approach. This means that the fundamental rights implications present in the project are also considered even where those concerns relate to private actors in the consortium. This is in line with the '*protect, respect, remedy'* framework suggested by Ruggie in the UN Guiding Principles of Business

[164] TRI, CAP, and INTERPOL then divided up the most relevant rights into groups and analysed them. TRI evaluated: Human dignity; Right to the integrity of the person; Prohibition of torture and inhuman or degrading treatment or punishment; Right to liberty and security; Respect for private and family life; Protection of personal data; Freedom of Expression and Information; Freedom of assembly and association.
INTERPOL considered rights of: Non-discrimination; Cultural, religious and linguistic diversity; Equality between men and women; The rights of the child; The rights of the elderly; Integration of persons with disabilities.
CAP analysed the: Right to an effective remedy and a fair trial; Presumption of innocence and right of defence.

[165] LED

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

and Human Rights. Following this, state actors should protect rights and provide remedy for violations of them. Private actors should respect rights, meaning they should act as if they are legally obligated to protect them, even where they are not, and mitigate the human rights impacts of their business practices.[166] In order to fulfil this approach, human and fundamental rights concerns that could be raised during the project are discussed and partners are encouraged to abide by them.

In terms of the scenarios, TRI developed initial scenario sketches which were then discussed with INTERPOL and CAP and edited to take the discussions into account. These are provided following the analysis below. Following an integrated webinar, the scenarios will be distributed to both internal and external attendees for feedback. As with the scenarios in T3.2, they have been created in order to expose the issues so that potential solutions can be suggested.

With regard to dissemination of the analysis, a summarised form of the below information will be sent to: interested parties in the INTERPOL LEA network; policymakers such as the European Parliament Intergroup 'Artificial Intelligence and Digital', the European Parliament Committee on Legal affairs, the European Parliament Committee on Civil Liberties, Justice, and Home Affairs, and; civil society organisations who engage in work on topics of technology and organised crime, such as Panoptykon,[167] Centre for Evidence Based Crime Policy,[168] The Royal United Service Institute,[169] Chatham House,[170] The Police Foundation ,[171] Centre for European Policy Studies .[172]

4.1. Fundamental rights analysis

The analysis of each right offered below first defines each right that is thought to be relevant to ROXANNE, and then explains the nature of the right. Next, the relevance of the right to the development and use of the project are explained.

Article 1 - Human dignity

This right is explained in the EU Charter as: '*Human dignity is inviolable. It must be respected and protected*.'

In human rights terms, 'dignity' is seen as a foundation of rights and a right in itself.[173] Thus, it is difficult to define. Article 1 is generally used to refer to the freedom to shape one's life,[174] and to reinforce other rights where people have been subjected to specific indignities.[175] This has particularly been the case in terms of: workers in situations where free movement is threatened;[176] protection of minors in relation to advertising in audiovisual and information services;[177] minimum standards for reception of asylum seekers;[178] detention of

[166] Ruggie, John, *guiding Principles on Business and Human Rights*, United Nations Office of the High Commissioner for Human Rights, New York and Geneva, 2011, p.13.
[167] Panoptykon Foundation, Home, 2020. Available at: https://en.panoptykon.org/
[168] Centre for Evidence Based Crime Policy, Home, George Mason University, 2020. Available at:https://cebcp.org/
[169] The Royal United Services Institute, Organised Crime, 2020. Available at:https://rusi.org/projects/organised-crime
[170] Chatham House, Drugs and Organised Crime, 2020. Available at:https://www.chathamhouse.org/topics/drugs-and-organized-crime
[171] The Police Foundation, Home, 2020. Available at: http://www.police-foundation.org.uk/
[172] Centre for European Policy Studies, Justice and Home Affairs, 2020. Available at: https://www.ceps.eu/ceps-unit/justice-and-home-affairs/
[173] Explanation on Article 1 – Human Dignity, Explanations Relating to the Charter of Fundamental Rights, OJ C303/17, 14.12.2007 (hereafter: CFR Explanations).
[174] Catherine Dupré 'Article 1' in Steve Peers, Tamara Hervey, Jeff Kenner, and Angela Ward (eds.), 'The EU Charter of Fundamental Rights: A Commentary' (Hart Publishing, 2014) (hereafter: Dupré, 2014), para.01.06.
[175] Dupré, 2014, para.01.29; also see Pretty v UK App No 2346/01 (ECtHR, 29 July 2002)
[176] Recitals (5) and (15), Directive 2004/38/EC of the European Parliament and of the Council, 29 April 2004, on the right of citizens of the EU and their family members to move and reside freely within the territory of the Member States.
[177] Arts. 2a and 3e, Recitals 37, 44, 45, 47, 53 and 67, Directive 2007/65/EC of the European Parliament and of the Council

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

third-country nationals;[179] equality between men and women (in employment and training); [180] biotechnology.[181]

Relevance to the project and use

It is unlikely that there will be direct effects on the freedom of people to shape their lives emanating from either the ROXANNE project, or its use. Of course, use of ROXANNE will likely advance criminal investigations and a criminal being put in prison will affect their freedom to shape their life, but that is a legitimate interference with their rights and so should not affect the use of ROXANNE (or any other LEA technology) specifically. However, scholars and activists have argued that human dignity is a foundational basis for privacy[182] and the European Data Protection Supervisor has suggested that "better respect for and safeguarding of human dignity could be the counterweight to pervasive surveillance and asymetry of power which now confronts the individual".[183] In this view, large scale personal data processing can itself potentially pose a threat to human dignity.

In terms of Article 1 reinforcing other rights, this could be an issue if violations of other rights occur and their violation causes a particular indignity. As such, the relevance of this aspect of this right to human dignity can only be assessed in relation to other rights discussed below.

Article 3 – Right to the integrity of the person

This right is defined as:

> '*1. Everyone has the right to respect for his or her physical and mental integrity.*
>
> *2. In the fields of medicine and biology, the following must be respected in particular:*
>
> - *the free and informed consent of the person concerned, according to the procedures laid down by law,*
> - *the prohibition of eugenic practices, in particular those aiming at the selection of persons,*
> - *the prohibition on making the human body and its parts as such a source of financial gain,*
> - *the prohibition of the reproductive cloning of human beings.*'

of 11 December 2007 amending Council Directive 89/552/EEC on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the pursuit of television broadcasting activities.

[178] Recitals 18 and 35, Directive 2013/33/EU of the European Parliament and of the Council of 26 June 2013 laying down standards for the reception of applicants for international protection; Recital 5, Council Directive 2003/9/EC of 27 January 2003 laying down minimum standards for the reception of asylum seekers.

[179] Art.8, Recital 2, Directive 2008/115/EC of the European Parliament and of the Council of 16 December 2008 on common standards and procedures in Member States for returning illegally staying third-country nationals.

[180] Art.2, Directive 2006/54/EC of the European Parliament and of the Council of 5 July 2006 on the implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation (recast); Case C-13/94 *P v S and Cornwall Council* [1996] ECR I-2143.

[181] Recitals 16 and 38, Directive 98/44/EC of the European Parliament and of the Council of 6 July 1998 on the legal protection of biotechnological inventions.

[182] Floridi, L. On Human Dignity as a Foundation for the Right to Privacy, Philos. Technol.29, 307–312 (2016). https://doi.org/10.1007/s13347-016-0220-8;Privacy International "It's about human dignity and autonomy", 12 July 2018, https://privacyinternational.org/long-read/2208/its-about-human-dignity-and-autonomy,

[183] European Data Protection Supervisor (2015), 'Opinion 4/2015 Towards a New Digital Ethics Data, Dignity and Technology'

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

This article relates primarily to health,[184] including mental suffering, anxiety, indignity, and humiliation.[185] This right is based upon Article 26 of the European Convention on Human Rights and Biomedicine that be restricted in the interest of public safety, prevention of crime, the protection of public health, or for the protection of the rights and freedoms of others.

Relevance to the project

During the project, this right has relevance to the use of human participants in research activities. Although paragraph (2) of this Article explicitly refers to the fields of medicine and biology, it is worth conserving the legal rules therein due to the use of human participants in ROXANNE. As explained in D10.1 (Procedures for identifying/recruiting research participants) and D10.7 (Informed consent procedures), human participation in the project includes asking volunteers to respond to surveys, provide a voice recording, or partake in interviews/workshops. All participants are asked to give informed consent before participating, both as a matter of research ethics, and as a legal basis for the processing of participant's personal data. Further, as noted in D10.2 (Opinions of ethics committees), these activities have been approved by an ethics committee; there will be no activities involving eugenics, financial gain, or cloning.

In terms of respecting physical and mental integrity, participants should not be subject to anything that would harm their physical or mental health. Meaning that, in the context of research, persons should not be subjected to unwanted medical treatments or physical invasion of one's body.[186] In the ROXANNE project, no participants will be subject to any form of medical research: they will only be used as sources of data recorded through writing or speaking – there will not need to be any physical contact between researchers and participants. As such, this part of the right is not applicable to the ROXANNE project.

Requirement not to impair the physical integrity of human participants in research completed.

With regard to mental integrity, this relates to freedom from psychological pressure and the imposition of mental suffering.[187] In order to prevent imparting any pressure or suffering, human participation in research should only take place where the person consents.[188] In order for consent to be valid, it must be informed, meaning that people should be '*fully informed*' about what is happening to them[189] through being '*given appropriate information as to the purpose and nature of the intervention as well as on its consequences and risks*'[190] and are able to make a free choice.[191]

Consequently, where persons are provided with appropriate information about what they are consenting to and are given a real opportunity to choose whether to give (or withdraw) consent, this would seem to be in accordance with this right. The ROXANNE partners will give all participants detailed information sheets prior to any research activity involving human beings, and participants will be expected to sign an informed consent form prior to beginning the activity. They will be free to not give consent, and to not partake in the activity, and will also be free to withdraw from the activity at any time without negative consequences; participants are informed of this on the information sheets.

Requirement not to impair the mental integrity of human participants in research completed.

[184] Sabine Michalowski, 'Article 3', in Steve Peers, Tamara Hervey, Jeff Kenner, and Angela Ward (eds.), 'The EU Charter of Fundamental Rights: A Commentary' (Hart Publishing, 2014) (hereafter: Michalowski, 2014), para.03.01.

[185] See Jalloh v Germany App no 54810/00 (ECtHR, 1 July 2006)(hereafter: Jalloh, 2006); Dordevic v Croatia App no 41526/10 (ECtHR, 24 July 2012) (hereafter: Dordevic, 2012)

[186] Jehovah's Witnesses of Moscow v Russia App no 302/03 (ECtHR, 10 June 2010) (hereafter: Jehovah's Witnesses, 2010), p.135; Pretty v UK App no 2346/02 (ECtHR, 29 April 2002) p.63.

[187] Michalowski, 2014, para.03.20; Jalloh, 2006, para.79

[188] Jehovah's Witnesses, 2010, p.135.

[189] V.C. v Slovakia App No 18968/07 (ECtHR, 8 November 2011) (hereafter: V.C. case, 2011), p.112.

[190] Art.5, Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine (adopted 4 April 1997, entered into force 1 December 1999) 2137 UNTS 171.

[191] V.C case, 2011, p.115.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

Relevance to use

The ROXANNE platform is designed to be used by LEAs to analyse data during organised crime investigations. Consequently, paragraph (2) of this Article is not applicable to the use of the ROXANNE platform.

As the ROXANNE platform will be analysing data collected by LEAs, actual use of the platform does not require physical contact between LEA officers and suspects. Consequently, use of the platform is unlikely to have any direct impact upon the physical integrity of persons.

> *Recommendations for LEAs to not impair the physical integrity of surveillance subjects when using the ROXANNE platform.*

In terms of mental integrity, it is unlikely that persons investigated by LEAs will be aware that they are being subjected to data analysis using the ROXANNE platform. As such, it is difficult to see how they could have their mental integrity affected. However, it is not unimaginable that a suspect might find out that they were under surveillance if they are informed of this during the court process. This could, potentially, lead to feelings of mental suffering, anxiety, indignity, and humiliation.[192] The European Court of Human Rights requires states to implement legal frameworks with enforcement mechanisms to protect the psychological integrity of persons.[193] As the intended market for ROXANNE is in Europe, the expected end-users will likely have already implemented such measures. If not, then they should be put in place before using ROXANNE. In any case, it is likely that any interference with this right could be lawful in situations where placing a suspected criminal under surveillance is necessary and proportionate to investigate or prevent criminality.

> *Recommendation for LEAs to enact measures to protect the psychological integrity of surveillance subjects if they experience mental suffering following disclosure that they were under surveillance.*

Article 4 - Prohibition of torture and inhuman or degrading treatment or punishment

This right is defined as: '*No one shall be subjected to torture or to inhuman or degrading treatment or punishment.*'.

It has the same wording, meaning and scope as Article 3 of the European Convention,[194] by virtue of Article 52(3).

This article relates to both physical and mental suffering.[195] Torture requires deliberate infliction of severe pain or suffering upon a powerless person who is under the physical custody or control of the torturer for a specific purpose.[196] Inhumane treatment requires 'severe' suffering, where one of the intention, purpose, or powerlessness of the victim, is missing (physical control is not necessary).[197] Degrading treatment is the infliction of pain or suffering in a particularly humiliating manner.[198]

[192] See, for example, Jalloh 2006,, p79.; Dordevic, 2012, p.95.

[193] And physical integrity also, see A, B, and C v Ireland App No 25579/05 (ECtHR, 16 December 2010), p.245.

[194] Explanation on Article 4 - Prohibition of torture and inhuman or degrading treatment or punishment, CFR explanations.

[195] See Art.1, Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (adopted 26 June 1987, entered into force 26 June 1987) 1465 UNTS 85; Art.7(2)(e), Rome Statue Of The International Criminal Court 1998 (adopted 17 July 1998, entered into force 1 July 2002) 2187 UNTS 3.

[196] Manfred Nowak and Anne Charbord, 'Article 4', in Steve Peers, Tamara Hervey, Jeff Kenner, and Angela Ward (eds.), 'The EU Charter of Fundamental Rights: A Commentary' (Hart Publishing, 2014) (hereafter: Nowak and Charbord, 2014), para.04.38.

[197] Nowak and Charbord, 2014, para.04.38.

[198] Nowak and Charbord, 2014, para.04.38.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

Relevance to the project

During the project it is unforeseeable that an individual could be subjected to severe pain or suffering. Research participants will be asked to engage in surveys, interviews, and workshops, none of these will require direct physical interaction between the participant and the researcher, and so physical pain cannot be caused. It is possible that a participant could feel uncomfortable during their participation, if they feel that an interview question is particularly probing, for example. However, merely feeling uncomfortable is not on the same level as acts prohibited under Article 3, which are characterised by their severity.[199] As such, it is extremely unlikely that a human participant in the ROXANNE project would experience such suffering and, in all cases, they are free to withdraw from their participation at any time without negative consequences.

In terms of colleagues within the ROXANNE consortium, it is extremely unlikely that anyone would experience suffering at this level, even if, for example, one colleague subjected another to bullying behaviour. Although bulling is a very difficult experience, it would not generally seem to approach the severity of torture or inhuman treatment. In any case, consortium partners have agreed[200] to abide by the European Charter for Researchers, which requires that '*individuals and research groups are valued, encouraged and supported*'.[201] As such, any behaviour approaching bullying, or worse, would seem to violate this requirement and so could result in sanctions such as loss of funding or election from the project.

Consequently, it is not conceivable that human participants, or colleagues, in the ROXANNE project would suffer torture, inhuman, or degrading treatment. As such this Article would seem to be complied with.

Requirement for partners to avoid causing severe suffering to colleagues completed.

Relevance to use

As with rights to the integrity of the person, it is *prima facie* difficult to conceptualise how the use of ROXANNE as a platform processing surveillance data can have real impacts upon criminal suspects. As with that right, harms could be created where suspects find out that they are under surveillance and the potential for mental distress to be caused by revelations during a court case that they were under surveillance. Although learning such information could be disturbing, it is unlikely to create the severity of harm equivalent to torture. Still, it is worth considering the possibility that as the analysis tools of ROXANNE could provide deeper insights into a person's life by exposing their acquaintances and contacts, more harm could be caused than discovering that oneself is under 'ordinary' surveillance. Still, the discomfort of having information about themselves and their friends and family in the network analysis part of the ROXANNE platform is unlikely to rise to the prohibited level of severe suffering. In authoritarian regimes that do deploy torture for political aims, such a network analysis tool could contribute to this situation. E.g., identifying people connected to political dissidents then threatening them, or exposing them to the risk of torture or abuse. The threat to the right however, comes from the act of torture itself.

Recommendation for LEAs not to use the ROXANNE platform to cause severe suffering to individuals.

Article - 6 Right to liberty and security

This right is defined as: '*Everyone has the right to liberty and security of person*'.

[199] Manfred Nowak, Report of the Special Rapporteur on torture and other cruel, inhuman or degrading treatment or punishment (Human Rights Council, 13th Session) 2010, A/HRC/13/39/Add.5, paras.50-57.
[200] Art. 32.1, ROXANNE Grant Agreement.
[201] Commission Recommendation 2005/251/EC of 11 March 2005 on the European Charter for Researchers and on a Code of Conduct for the Recruitment of Researchers, OJ L 75, 22.3.2005.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

It has the same meaning and scope as Article 5 of the European Convention[202] by virtue of Article 52(3). Thus, although the limitations within Article 5 of the Convention apply to the application of Article 6 of the Charter, even though they are not specifically included in the Charter itself:

> *'1. Everyone has the right to liberty and security of person. No one shall be deprived of his liberty save in the following cases and in accordance with a procedure prescribed by law:*
>
> *(a) the lawful detention of a person after conviction by a competent court;*
>
> *(b) the lawful arrest or detention of a person for non-compliance with the lawful order of a court or in order to secure the fulfilment of any obligation prescribed by law;*
>
> *(c) the lawful arrest or detention of a person effected for the purpose of bringing him before the competent legal authority on reasonable suspicion of having committed an offence or when it is reasonably considered necessary to prevent his committing an offence or fleeing after having done so;*
>
> *(d) the detention of a minor by lawful order for the purpose of educational supervision or his lawful detention for the purpose of bringing him before the competent legal authority;*
>
> *(e) the lawful detention of persons for the prevention of the spreading of infectious diseases, of persons of unsound mind, alcoholics or drug addicts or vagrants;*
>
> *(f) the lawful arrest or detention of a person to prevent his effecting an unauthorised entry into the country or of a person against whom action is being taken with a view to deportation or extradition.'*

This article relates to the ability of persons to freely move in physical space.[203] Although the form of a deprivation of liberty should be interpreted widely,[204] it is focussed on the right not the be detained arbitrarily.[205]

Relevance to the project and use

It is unforeseeable that a research participant or colleague would be physically detained in any way as part of their engagement with the project. As such it is not relevant to the project.

In terms of use, it is also difficult to consider that the use of a platform intended to analyse surveillance data could have a direct effect on the ability physical liberty of a person. However, it is worth considering whether the effect of surveillance and LEA data analysis could affect the liberty of suspects. For example, if someone were to be aware they were at risk of having their data analysed by a ROXANNE-like system, then this would likely create 'chilling effects' where people change their behaviour owing to the (risk of) coming to the attention of LEAs as, in order to avoid punishment, the only 'rational' option is to follow the expectations of the LEA.[206] Such concerns are relevant to the ROXANNE platform as people are likely to want to shield their associates whom they are in communication networks with. The manifestation of such effects could have significant impacts upon how much liberty people feel they have. For example, some people may stop exercising their liberty. However, even if people do feel constrained in their behaviours owing to (a risk of) being analysed by ROXANNE, the article relates to physical liberty only. As the use of a surveillance data analysis platform does not directly affect the physical liberty of the surveillance subjects, this article is not directly related to the use of the ROXANNE platform.

We can however anticipate a situation where outputs from such a data analysis platform contribute towards suspicion that an offence has taken place, thus leading to the arrest and detention and subsequent loss of liberty of a suspect. If the outputs of the platform and tools are false, erroneous, have been insufficiently tested, or are

[202] Explanation on Article 6 - Right to liberty and security, CFR Explanations.
[203] De Tommaso v Italy App No. 43395/09 (ECtHR, 23 February 2017), para.80.
[204] Guzzardi v Italy App No 7367/76 (ECtHR, 6 November 1980), para.95.
[205] Daniel Wilsher, 'Article 6', in Steve Peers, Tamara Hervey, Jeff Kenner, and Angela Ward (eds.), 'The EU Charter of Fundamental Rights: A Commentary' (Hart Publishing, 2014)(hereafter: Wilsher, 2014), para.06.14.
[206] Lyon, David., *The Electronic Eye*, University of Minnesota Press, Minneapolis, 1994, p.63.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

based upon poorly understood mechanisms, then the platform potentiality contributes to unlawful arrest and the deprivation of liberty. This creates an obligation upon the project to ensure high quality science, rigorous testing, and proper communication around the outputs of the tools and how they can be misleading.

> *Requirement to respect people's right to liberty and security likely to be complied with if the project meets high standards of scientific research and its tools and platform are properly tested.*

Article 7 - Respect for private and family life

This right is defined as: '*Everyone has the right to respect for his or her private and family life, home and communications*'.

The meaning and scope of this right are the same as those in Article 8 of the European Convention (although 'correspondence' has been updated to 'communications'),[207] by virtue of Art.52(3) of the Charter. Consequently, the limitation on the right in the Charter correspond to those in the Convention:

> *'2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others'*

Owing to the nature of this right, it is seen to have two separate limbs: private life aspects and family life aspects. Clearly, the processing of speech, text, and video data gathered by surveillance can affect both aspects, and the use of network analysis could be used to infer information across both aspects also. As such, ROXANNE could pose a particular challenge to this right.

Regarding the private life aspect, it is interpreted widely and also relates to one's home life and communications. It is focussed upon protecting activities of a personal nature, such as names, personal identity, and one's home.[208] These data are protected whether or not they have been processed.[209] This has links with the family life aspect as a person's name provides familial information.[210] Further, the private life aspect includes professional life as far as one's professional life is also part of one's home life.[211] For example, where one's home is also one's business premises.[212]

The family life aspect is interpreted widely.[213] It is focussed on gender equality,[214] children's rights,[215] free movement, immigration, and asylum.[216]

Relevance to the project

The work of the ROXANNE project does not seem to raise any of the issues mentioned in Article 7 for colleagues or research participants: personal contact details will only be gathered where the individual

[207] Explanation on Article 7 – Respect for private and family life, CFR Explanations.

[208] Jens Vedsted-Hansen, Article 7 (Private Life, Home and Communications), in Steve Peers, Tamara Hervey, Jeff Kenner, and Angela Ward (eds.), 'The EU Charter of Fundamental Rights: A Commentary' (Hart Publishing, 2014)(hereafter: Vedsted-Hansen, 2014), para.07.23A-07.24A, 07.66A-07.73A

[209] Vedsted-Hansen, 2014, para.07.21A-.7022A

[210] Vedsted-Hansen, 2014, para.07.24A

[211] Vedsted-Hansen, 2014, para.07.08A

[212] Vedsted-Hanson, 2014, para.07.11-07.20A

[213] Shazia Choudhry, Article 7 (Family Life Aspects), in Steve Peers, Tamara Hervey, Jeff Kenner, and Angela Ward (eds.), 'The EU Charter of Fundamental Rights: A Commentary' (Hart Publishing, 2014)(hereafter: Choudhry, 2014), para.07.20B

[214] Choudrhy, 2014, para.07.02B-07.04B

[215] Choudhry, 2014, para.07.05B-07.06B

[216] Choudhry, 2014, para.07.07B-07.09B

concerned willingly provides them; no communications between persons will be monitored; there will be no interference in any person's family life.

Yet, there is a possibility that the project could process LEA surveillance data from real closed cases in order to test a prototype ROXANNE platform. If this happens, only lawfully gathered data would be acceptable for use. Of course, gathering these data in criminal investigations is a situation where respect for a persons' private and family life is clearly relevant. Thus, in order for it to have been gathered in compliance with this Article, any such surveillance data would need to have been collected in accordance with domestic law, and for it to have been necessary for one of the limitations provided in paragraph 2 to apply; in the case of ROXANNE, this is most likely to be '*for the prevention of disorder or crime'*. Where this is the case, the infringement on the private and family lives of persons during an investigation is not arbitrary and the Article is complied with.

The re-using of surveillance data for research purposes would seem to be a separate situation where there is potential for infringing upon the respect for private and family life. Data gathered by surveillance is, by its nature, sensitive, and so all processing activities of it seem to raise a risk of infringing upon this right. Thus, in order for the processing of these data in the ROXANNE project to not violate Article 7, the same test as mentioned above would need to be applied. As mentioned above, LTEC are the only LEA who have expressed an intention to process data from real closed cases, and have confirmed that these data were gathered lawfully.

> *Requirement for LEA officers to ensure any data made available to be used in the project was gathered lawfully, completed so far.*

For such processing to be in conformity with domestic law, it must be processed according to applicable data protection legislation, i.e. the GDPR and the relevant national implementing legislation. No data processing in the ROXANNE project will take place contrary to the GDPR, and so this part of the test will be fulfilled. By contributing to a project building new tools to assist in fighting organised crime and terrorism, such processing clearly contributes to the '*prevention of disorder or crime'*, and so this part of the test is also met. In terms of whether these activities are necessary in order to prevent disorder or crime, the European Court has stated that there must be a '*pressing social need*'[217] as understood by each state within a margin of appreciation.[218] The ROXANNE project responds to the difficulties experienced by LEAs in large organised crime investigations, and potentially solving or reducing these difficulties would seem to meet a pressing social need. The fact that LEA partners are permitted by their governments to participate in projects such as ROXANNE indicates that their states view their participation as contributing to a pressing social need also. Consequently, any interference with an individuals right to privacy experienced through the use of their data in the ROXANNE project could in compliance with the right. Having said that, the 'need' for real closed case data must be evaluated. Partners need to consider if it would be possible to test the ROXANNE platform using data that is less sensitive and not from real closed cases. As mentioned above, LTEC consider that use of synthetic data would risk misjudging the accuracy and capabilities of the platform.

> *Requirement to respect the private and family life of data-subjects by considering if other, less-sensitive, data sources that real closed case data are available, completed so far.*

Relevance to use

The potential for the use of ROXANNE to infringe upon a person's right to privacy would seem to be the same as any other machine used in surveillance by LEAs: its use would need to be in compliance with domestic law and necessary for, and proportionate to, the prevention of disorder or crime. In the current situation, tools used for identifying persons in surveillance data are used separately from network analysis tools, and investigators can assess the need for both activities separately. As ROXANNE brings both technologies together, this creates a requirement that the platform does not automatically run data through both types of tools as it might be necessary only to use one. For example, it might be necessary to identify a suspected criminal in an investigation, but not necessary to map their communication network.

[217] Dudgeon v The United Kingdom App No 7525/76 (ECtHR, 22 October 1981), para.51.
[218] Paradis and Campanelli v Italy App No 25358/12 (ECtHR, 24 January 2017), paras.179-184.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

> *Requirement for technical partners to build the ROXANNE platform in such a way that data is not automatically subject to both recognition and network analysis technologies, not yet possible to evaluate.*

It is particularly important that LEA officers consider the effects of subjecting investigative data to analyses for the purposes of both individual and network identification as the interference with communications between a suspected criminal and another person are an infringement on the privacy of both persons.[219] As such, in order to analyse surveillance data that includes persons other than the suspect, it must also be necessary to infringe on the privacy of these innocent persons. With network analysis, this could be a large number of persons and so it could be difficult to assess the necessity of infringing on the privacy of every person, and whether the test should be applied to each person individually or the data-set as a whole. It would be insufficient simply to extend analysis to the data of other persons because they are merely '*involved in a criminal offence*',[220] indeed the European Court requires that precautions to protect persons who are incidentally recorded must be enacted in domestic law.[221] Thus, in order to be lawful, the extension of criminal network analysis to the associates of a suspected criminal must have a basis in domestic law, which is specific enough to so that the persons who could be subjected to surveillance could be determined.[222] The functionality should be built into the tool that requires the user to provide or record their basis in national law before they can use the tool.

> *Recommendation for LEAs to only use ROXANNE tools to infringe upon the privacy of persons where it is provided for in domestic law.*
>
> *Requirement for technical partners to enable LEAs to attest to their lawful use of data, not yet possible to evaluate.*

Article 8 - Protection of personal data

This right is defined as:

> '*1. Everyone has the right to the protection of personal data concerning him or her.*
>
> *2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*
>
> *3. Compliance with these rules shall be subject to control by an independent authority.*'

Paragraph 1 of this Article comes from Article 16(1) of the Treaty of the Functioning of the European Union. With regard to secondary legislation, the EU has developed a range of instruments relating to personal data. The most relevant of these are the General Data Protection Regulation (GDPR), and the Law Enforcement Directive (LED).

The Charter is unique in that there is no corresponding right to the protection of personal data under other human rights treaties. This is despite the fact that data protection legislation itself provides rights to data subjects for specific instances (e.g. access,[223] rectification,[224] erasure[225]).

However, in other human rights regimes, the protection of personal data is considered to form part of rights to privacy.[226] For example, in assessing data privacy, the ECtHR has considered: the nature of the data;[227] the

[219] Lambert v France App No 23618/94 (ECtHR, 24 August 1998), para.21.
[220] Iordachi and Others v Moldova App No 25198/02 (ECtHR, 14 September 2009), para.44.
[221] Amann v Switzerland App No 27798/95 (ECtHR, 16 February 2000), para.61.
[222] Amann v Switzerland App No 27798/95 (ECtHR, 16 February 2000), para.61.
[223] Art.15, GDPR
[224] Art.16, GDPR
[225] Art.17, GDPR
[226] European Union Agency for Fundamental Rights, *Handbook on European data protection law*, FRA, Luxembourg,

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

privacy expectation of the person concerned;[228] access of the person concerned to data;[229] the presence of oversight mechanisms;[230] whether security measures have been put in place.[231] A case-by-case approach is taken by the European Court, and so the precise contours of how the protection of personal data is dealt with under the right to a private life can only be foreseen generally.

The right to protection of personal data in the EU Charter is not absolute, '*but must be considered in relation to its function in society*.'[232] Limitations on this right are recognised under Art.52(1) of the Charter. They must be provided for by law, respect the essence of the right, and be proportionate, necessary, and meet legitimate objectives.[233] The same approach is taken in relation to personal data forming part of ones privacy in other human rights regimes.[234]

Relevance to the project

The processing of personal data in the ROXANNE project is subject to the GDPR. As such, processing that is in line with this, or national implementing legislation, is provided for by law. The essence of the right is respected by using anonymous or pseudonymous data where possible, and preferring to process personal data on the basis of consent. Processing of personal data in the project is proportionate to the aim of conducting scientific research as there will be no effects created for data subjects, and nor will there be any combining of datasets with the intention to uncover highly-sensitive information about data-subjects. The processing of personal data in the project is necessary as it would not be possible to produce the intended algorithms without training them on personal data. Scientific research is a legitimate objective as, by its nature, it results in greater knowledge and advancement for society and in the case of ROXANNE, contributes to the increased safety of citizens from organised criminal gangs.[235]

Requirement for the project to comply with data protection legislation likely to be complied with.

Relevance to use

The processing of personal data during potential use of the ROXANNE platform in criminal investigations within the EU will be subject to the Law Enforcement Directive. Consequently, processing that is in conformity with this Directive, and national implementing legislation, would be provided for by law. Whether processing of personal data by LEAs is necessary and proportionate to meet a legitimate objective will depend upon the context of the investigations that are taking place. However, the ROXANNE consortium intends that any exploitation of the platform that involves its sale will only take place to organisations and countries who respect applicable human rights law and do not abuse their powers; as such, the consortium assumes that end-users will comply with the law during their usage of the platform. The platform should provide the functionality for users to be able to attest that their use of the tool is in line with their national legislation and operational procedures (for example, by recording an authorisation, or by self-attesting that they have the appropriate authorisation, without this, the tool should not be able to be used). Another supporting functionality would be for the tool to

2018, pp.17-18.

[227] Z v Finland App no 22009/93 (ECtHR, 25 February 1997)

[228] Krone Verlag GmbH v Austria App no 431/96 (ECtHR, 26 February 2002); Von Hannover v Germany App no 59320/00 (ECtHR, 24 June 2004)

[229] Leander v Sweden App no 9248/81 (ECtHR, 26 March 1987); Gaskin v UK App no 10454/83 (ECtHR, 7 July 1989), para.49

[230] Klass v Germany App no 5029/71 (ECtHR, 6 September 1978)

[231] I v Finland App no 20511/03 (ECtHR, 17 July 2008), para.38-40

[232] CJEU, Joined cases C-92/09 and C-93/09, Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen [GC], 9 November 2010 (hereafter: Land Hessen, 2010), para. 48.

[233] Land Hessen, 2010, para.51

[234] See, for example, Article 8, European Convention for the Protection of Human Rights and Fundamental Freedoms (adopted 4 November 1950, entered into force 3 September 1953) 213 UNTS 221.

[235] On Scientific research being a legitimate objective for data processing, see Recitals 156-158, GDPR. For a specific articulation of this for ROXANNE, see D10.7 (Informed Consent Procedures) and other completed ethics requirements..

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

allow users to record the output of a necessity and proportionality assessment or to record their rationale for the use of the tool, to discourage fishing for evidence and to allow accountability and auditability of the use of the tool within the end-user organisation.

> *Requirement for technical partners to facilitate end-users demonstrating compliance with data protection legislation prior to use, not yet completed.*

Article 11 – Freedom of expression and information

This right is defined as:

> *'1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.*
>
> *2. The freedom and pluralism of the media shall be respected.'*

This article corresponds to Article 10 of the European Convention, which provides greater detail:

> *'1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.*
>
> *2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.'*

Due to Article 52(3) of the Charter, the meaning and scope of Article 11 of the Charter are the same as Article 10 of the Convention. 'Expression' covers a range of actions beyond just speech,[236] including silence.[237] It applies whatever medium of communication is used, including oral, written, printed, and electronic forms.[238] Indeed, the freedom of expression '*applies not only to the content of the information but also to the means of transmission or reception since any restriction imposed on the means necessarily interferes with the right to receive and impart information.'*[239] As such, a speaker (broadly conceived) has a right to make information available a recipient has the right to receive that information.[240]

Relevance to the project

In terms of the ROXANNE project, it is unlikely that anyone's freedom of expression could be infringed upon. Partners partake in bi-weekly meetings where they can express their views in an open forum, they are, therefore, provided with opportunity to express and receive information. Participants in research activities are asked to express information, particularly in activities such as workshops and interviews where the project is specifically seeking interviewees to express themselves.

[236] Hasham and Harrup v the United Kingdom App No 25594/94 (ECtHR, 25 November 1999).
[237] K v. Austria App No 16002/90 (ECtHR, 13 October 1992), para.45.
[238] Case C-316/09 MSD Sharp & Dohme GmbH v Merckle GmbH, CJEU, Opinion of AG Trstenjak 24 November 2010, para.81.
[239] Neij and Sunde Kolmisoppi v. Sweden App No 10397/12 (ECtHR, 19 February 2013), dec.
[240] Mavlanov and Sa'di v Uzbekistan U.N. Doc. CCPR/C/95/D/1334/2004 (HRComm, 19 March 2009, para.6.1.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

Requirement to respect freedom of expression in the project likely to be completed.

Relevance to use

As a data-analysis (including voice, and speaker analysis) platform, ROXANNE would not have a direct impact on anybody's freedom of expression. However, there is potential that chilling effects could be created if an individual fears that their speech data is (at risk of) being analysed by LEAs using a platform such as ROXANNE, and they do not express themselves in order to avoid being included in this analysis for fear of being identified as a criminal. The freedom of expression protects all expression of information, apart from hate speech and incitement of violence.[241] Thus, an individual could, potentially, not express themselves about a range of topics that they do not wish to be recorded expressing or identified from. Because such analysis would likely be covert, an individual has no way of knowing if their particular expression activity is under surveillance.

In a legitimate and lawful LEA investigation of an organised crime group, this could, potentially, infringe upon the freedom of expression of someone under investigation (or believes they are under investigation). The European Court has held that 'self-censorship' of one's own expression due to a fear of court proceedings can violate the freedom of expression where the proceedings were unnecessary.[242] Consequently, if a criminal self-censors their own expression due to a fear of court proceedings occurring as a result of their criminality, and those proceedings are necessary, then is unlikely that the freedom of expression would be violated. Arrests in order to bring someone before a competent authority are considered necessary.[243] Indeed it is likely to be seen as a form of deterring criminals from openly engaging in criminality. As such, this type of interference with the freedom of expression is unlikely to be unlawful.

Recommendation for end-users to respect freedom of expression when using the ROXANNE platform by only using it where necessary.

Article 12 - Freedom of assembly and association

This right is defined as:

> *'1. Everyone has the right to freedom of peaceful assembly and to freedom of association at all levels, in particular in political, trade union and civic matters, which implies the right of everyone to form and to join trade unions for the protection of his or her interests.*
>
> *2. Political parties at Union level contribute to expressing the political will of the citizens of the Union.'*

Paragraph 1 of this Article corresponds to Article 11 of the ECHR, which is more detailed:

> *'1. Everyone has the right to freedom of peaceful assembly and to freedom of association with others, including the right to form and to join trade unions for the protection of his interests.*
>
> *2. No restrictions shall be placed on the exercise of these rights other than such as are prescribed by law and are necessary in a democratic society in the interests of national security or public safety, for the prevention of disorder or crime, for the protection of health or morals or for the protection of the rights and freedoms of others. This Article shall not prevent the imposition of lawful restrictions on the exercise of these rights by members of the armed forces, of the police or of the administration of the State.'*

[241] Sürek v Tukey App no 24735/94 (ECtHR, 8 July 1999), para.36.

[242] Maegulev v Russia, App No 15449/09 (ECtHR, 8 January 2020).

[243] Art.5(1)(c), ECHR; Lawless v Ireland (No.3), App No 332/57 (ECtHR, 1 July 1961).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

Pursuant to Article 52(3) of the Charter, the meaning and scope of the right under the Charter is the same as that under the Convention.

Paragraph 2 of this Article corresponds to Article 191 of the Treaty establishing the European Community: '*Political parties at European level are important as a factor for integration within the Union. They contribute to forming a European awareness and to expressing the political will of the citizens of the Union*.'

This right is also based on Article 11 of the Community Charter of the Fundamental Social Rights of Workers:

> *'Employers and workers of the European Community shall have the right of association in order to constitute professional organisations or trade unions of their choice for the defence of their economic and social interests. Every employer and every worker shall have the freedom to join or not to join such organisations without any personal or occupational damage being thereby suffered by him.'.*

Generally, the freedom of assembly protects the right of people to peacefully gather and meet for political,[244] social,[245] communal,[246] cultural,[247] or religious/spiritual purposes,[248] whether in private or public and whether static or as a procession/march.[249] 'Association' here means an affiliation with a group that has a common goal,[250] not merely sharing the company of, or mixing socially with, others.[251]

The ROXANNE platform itself, as a data-analysis platform, cannot be used to directly interfere with the freedoms of assembly and association held by citizens. However, owing to the potential for people to be identified from video and audio data by the ROXANNE platform, and for this to be linked with communications networks, the implementation of ROXANNE could, potentially, have a significant chilling effect on the freedom of people to peacefully assemble/associate where they fear that they themselves, or people they communicate with, could be subjected to surveillance for their activities with others. The intelligence analysis capacities enhanced by the platform would also enhance these capacities if they were used in an inappropriate manner (e.g., illegal surveillance and disruption of legitimate political activists) so would contribute towards the impact of activities that could directly interfere with freedom of assembly and association.

Relevance to the project

The nature of the personal data-processing in the ROXANNE project is to use data either as a source of information for analysis by social scientists (e.g. interviews at field-tests), or as data to be used for developing algorithms by computer scientists. As such, there will be no direct effects upon data-subjects and so cannot create a specific chilling effect regarding freedom of assembly/association.

> *Requirement to respect freedom of assembly within the project complied with.*

Relevance to use

In terms of use, there is potential for a significant chilling effect to be created if, by knowing about the ROXANNE platform, people believe that they are subject to (a risk of) having their data analysed and being identified by LEAs. This effect is likely to be increased, where people are concerned that LEAs will be able to

[244] Navalnyy v. Russia App No 29580/12 (ECtHR, 15 November 2008), para.102; Friend, the Countryside Alliance and others v. the United Kingdom App No 16072/06 and 27809/08 (ECtHR, 24 November 2009), para.50.

[245] Emin Huseynov v. Azerbaijan App No 59135/09 (ECtHR, 7 August 2015), para.91.

[246] Djavit An v. Turkey App No 20652/92 (ECtHR, 9th July 2003)(hereafter: Djavit An, 2003), para.60.

[247] The Gypsy Council and Others v. the United Kingdom App No 66336/01 (ECtHR, 14 May 2001)(dec.).

[248] Barankevich v. Russia App No 10519/03 (ECtHR, 26 October 2007), para.15.

[249] Kudrevičius and Others v. Lithuania App No 37553/05 (ECtHR, 15 October 2015), para.91;Djavit An, 2003, para.56.

[250] Young, James and Webster v. the United Kingdom, App Nos 7601/76 and 7806/77 (ECommHR, 14 December 1979), para.167.

[251] McFeeley v. the United Kingdom App No 8317/78 (ECommHR, 15 May 1980), para.114; Bollan v. the United Kingdom App No 42117/98 (ECtHR, 4 May 2000) (dec.).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

find out who they communicate with using the ROXANNE network analysis tools, thus exposing their associates to potential LEA investigation.

The paradigmatic example of chilling effects in relation to freedoms of assembly/association is of LEA actions, directly or indirectly, inhibiting the freedom of people to engage in political activities, such as protests or trade union activities. LEA interest in protests has been determined by the European Court to have a chilling effect even where that interest is temporary,[252] or later shown to be mistaken,[253] and where LEAs act unlawfully to ban a protest.[254] For the European Court, the potential for chilling effects to be detrimental to the freedom of assembly should be considered in terms of whether their actions are proportionate.

Consequently, freedoms of assembly/association can be infringed upon if people are dissuaded from assembling/associating where they fear that their presence could have negative effects and this is deemed to be a disproportionate result of pursuing a legitimate aim. If, for example, people involved in political movements decline to attend legitimate protests or meetings due to, a risk of, their data being analysed by ROXANNE-like tools, their freedoms of assembly/association could be infringed upon. The most obvious solution to this, of course, would be to not sell or provide the ROXANNE platform to LEAs who use their powers to stifle legitimate political activities.[255]

However, as noted above, freedoms of assembly/association also extend to social, communal, cultural, and religious/spiritual gatherings. If, for example, a member of an organised crime group knew that they were at risk of surveillance and so stopped engaging in social events in order to protect their innocent associates, could this be an infringement on their freedom of assembly? Engaging in social and cultural activities are an important part of people's lives. But they are not essential, and so the choice of someone to not engage in them in order to avoid potential surveillance would not seem to be a disproportionate effect. Whether this could even be considered relevant to the freedom of assembly would, of course, depend upon whether these acts are too distant from LEA activities to be infringed upon by the LEAs themselves. It is unlikely that LEAs could be held to have infringed upon a person's right to assembly where an LEA has no contact wit an individual yet they decide not to attend social events due to a fear of being subject to surveillance or data-analysis.

Recommendation for end-users to respect freedom of assembly.

Articles 21 to 26 – Rights to non-discrimination

The ROXANNE project solutions and activities may have implications on fundamental rights such as the broad principle of non-discrimination and in relation to specific diversity aspects related to gender, culture, age or physical characteristics. Therefore, in the development of the ROXANNE platform and its subsequent use, it is important to be aware of any potential diversity and non-discrimination rights repercussions.

Article 21[256] of the EU Charter of Fundamental Rights prohibits "*any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other*

[252] Christian Democratic People's Party v. Moldova App No 28793/02 (ECtHR, 14 May 2006), para.77.

[253] Nurettin Aldemir and Others v. Turkey App Nos 32124/02, 32126/02, 32129/02, 32132/02, 32133/02, 32137/02 and 32138/02 (ECtHR, 2 June 2008), para.34; The United Macedonian Organisation Ilinden and Ivanov v. Bulgaria App No (ECtHR, 15 February 2006), para.135.

[254] Bączkowski and Others v. Poland App No 1543/06 (ECtHR, 24 September 2007), paras.66-68.

[255] For more on steps taken by the ROXANNE consortium to avoid sales of the platform to organisations who do not have a good track record of respecting human rights, see D10.16 (Report on risks of misuse and mass surveillance.

[256] Article 21 Non-discrimination

> Any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited.
>
> Within the scope of application of the Treaty establishing the European Community and of the Treaty on European Union, and without prejudice to the special provisions of those Treaties, any discrimination on grounds of nationality shall be prohibited.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

opinion, membership of a national minority, property, birth, disability, age or sexual orientation". Furthermore, the EU Charter of Fundamental Rights prohibits discriminatory treatment on additional grounds, safeguarding cultural, linguistics and religious diversity in Article 22[257], equality between men and women in Article 23[258], the rights of children (Article 24[259]) and elderly (Article 25[260]), as well as integration of persons with disabilities (Article 26[261]). In a similar vein, the Universal Declaration of Human Rights enshrines the equal entitlement of all human beings to the fundamental rights and freedoms in Article 2 (*"without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status")* and Article 7 *("All are equal before the law and are entitled without any discrimination to equal protection of the law. All are entitled to equal protection against any discrimination in violation of this Declaration and against any incitement to such discrimination").*

The Charter on Fundamental Rights applies to EU institutions and signatory members states when implementing EU law whilst the Universal Declaration of Human Rights is not legally binding. However, the Declaration does provide a shared global vision of protected fundamental rights as agreed by representatives from different legal and cultural backgrounds. These were incorporated in many national constitutions and legal frameworks, including the INTERPOL Constitution that requires the Organization to promote the widest possible mutual assistance between all criminal police authorities within the limits of the laws existing in the different countries and in the spirit of the Universal Declaration of Human Rights.[262]

Data bias

In the pursuit of the ROXANNE project's tasks and objectives, the consortium should ensure the respect of the general and specific provisions of the rights to diversity and non-discrimination throughout the different project stages and activities. First, at the research level, it is of uppermost importance that the datasets used for the development and testing of the algorithms do not contain any gender, age, language or racial bias. Existing research[263] highlights the significant dangers related to ethnic profiling and other discriminatory treatments when authorities employ innovative technical solutions, such as facial recognition systems, that were constructed on biased dataset. Therefore, in the framework of the work undertaken within Work Package 4 on data management,

[257] Article 22 Cultural, religious and linguistic diversity
The Union shall respect cultural, religious and linguistic diversity.

[258] Article 23 Equality between men and women
Equality between men and women must be ensured in all areas, including employment, work and pay.
The principle of equality shall not prevent the maintenance or adoption of measures providing for specific

[259] Article 24 The rights of the child

Children shall have the right to such protection and care as is necessary for their well-being. They may express their views freely. Such views shall be taken into consideration on matters which concern them in accordance with their age and maturity.

In all actions relating to children, whether taken by public authorities or private institutions, the child's best interests must be a primary consideration.

Every child shall have the right to maintain on a regular basis a personal relationship and direct contact with both his or her parents, unless that is contrary to his or her interests.

[260] Article 25 The rights of the elderly
The Union recognises and respects the rights of the elderly to lead a life of dignity and independence and to participate in social and cultural life.

[261] Article 26 Integration of persons with disabilities
The Union recognises and respects the right of persons with disabilities to benefit from measures designed to ensure their independence, social and occupational integration and participation in the life of the community.

[262] INTERPOL Constitution Article 2 https://www.interpol.int/Who-we-are/Legal-framework/Legal-documents

[263] « Data-driven policing : the hardwiring of discriminatory policing practices across Europe » Patrick Williams and Eric Kind ENAR, November 2019, https://www.enar-eu.org/IMG/pdf/data-driven-profiling-web-final.pdf
AI expert calls for end to UK use of 'racially biased' algorithms', The Guardian, 12 December 2019, https://www.theguardian.com/technology/2019/dec/12/ai-end-uk-use-racially-biased-algorithms-noel-sharkey

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

- due regard and consideration should be given to assessing the project-employed datasets for potential data biases. The technical partners should be vigilant and scrutinize any potential discriminatory implications of a particular dataset under consideration, notwithstanding if derived from open source channels such as YouTube, fabricated data created based on a LEA-provided scenario with partners engaging in role-play or based on existing synthetic or real datasets such as CSI and Enron. This should translate into avoiding over-reliance on particular languages, age, gender or ethnic categories as the end-product may perform better regarding these categories and result in profiling representatives of particular groups.
- Consultations with the project legal and ethical team could be useful to verify that the used datasets fulfill such requirements.
- Beyond the construction of computer models, their testing and appraisal (efforts pursued within the scope of Work Package 8) represent another crucial moment for identifying and managing inaccurate or discriminatory line codes in order to avoid producing a skewed project outcome.
- In this regard, the external expertise of the Stakeholder and Ethics Boards plays an important oversight role.

Requirement for technical partners to train and build the ROXANNE tools to avoid discriminatory biases to be evaluated.

Further in line with this objective, it is advisable to maintain a human-centric approach to the handling of advanced technological tools such as ROXANNE by keeping ultimate decision-making control in the hands of humans. This should be achieved by designing the technology accordingly to enable authorized human operators with an understanding of the underlying processes, to have the possibility to interfere and correct algorithms suspected of making biased or disproportionate results. For example, if after prolonged and repeated ingestion of investigative data containing lawfully intercepted telephone conversations in a particular foreign language, the platform may eventually end up targeting individuals speaking that particular language. A human operator of the system should be aware of such potential implications and maintain a critical interpretation of automatic decision-making results.

Requirement to maintain human control over the ROXANNE platform to be evaluated.

End-user requirements

Secondly, when analysing and defining the applicable end-user requirements, fair, impartial, inclusive and equal treatment should be given to the needs expressed by stakeholders coming from different backgrounds, i.e. operational units, forensics, country/culture wise, gender wise, etc. Given the value of expert feedback in designing feasible, realistic ROXANNE solutions that overcome current investigative shortcomings, the project team emphasized the importance of expert guidance and insight from the earliest stage and will continue this to the development of the finished ROXANNE product. This is reflected in the consortium's diversity, which contains 11 LEAs from 10 countries across Europe. The project Stakeholder Board provides an additional level of expertise and consultation with its 16 members representing 12 institutions such as the UN, Europol, EC policy-makers and national authorities. Besides, for the essential task of collecting end-user requirements from the law enforcement community, INTERPOL leveraged its international network of 194 member countries by reaching out to a diverse and truly global audience of stakeholders to provide their opinion and share their experiences on the use of voice, text and face technologies. This will enable the ROXANNE consortium to develop a solution tailored to the experiences and needs of LEAs by integrating insights coming from different professional and cultural backgrounds into the system design and development of the ROXANNE platform. Another key aspect in this regard is ensuring that all analysis of gathered feedback, performed within the scope of WP2 on end-user requirements and WP8 as part of continuous testing and field-tests, is conducted in an anonymous way in order to uphold the impartiality of the needs assessment. As mentioned above, analysis of feedback from the first field-test in D8.4 (1st field-test report and recommendations) incorporated feedback from a wide range of stakeholders and so the consortium is complying with the point so far.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

> *Requirement to treat all feedback on the ROXANNE platform fairly and without discrimination completed so far.*

Lawful operation

Thirdly, following the research phase into and the tools' commercialisation to competent police authorities, the eventual acquisition and use of the ROXANNE solutions must be compatible with applicable domestic and regional legislation and framed by organisational codes of use and standards. To this end, a well-thought and technically robust design of the ROXANNE platform secured during the project's development stage would enable a transparent and accountable use of the technology adaptable to national provisions. Although the reliance on novel analytical methods often lacks specific guidance, encouraging legislative, policy, and strategy developments are emerging in the area.[264] Furthermore, in the context of the exploitation planing discussion, as well as within meetings of the Ethics Boards, the project team has been considering the implications of the ROXANNE solutions' misuse, including safeguards for a non-discriminatory application of the ROXANNE tools. This could potentially occur should the tool land in the hands of authoritarian regimes or criminal groups that could use it to target vulnerable communities such as refugees or minority groups. Therefore, the consortium is currently in the process of considering commercialisation measures, such as 'know your customer' policies or conducting due diligence assessment, as well as contractual clauses that prohibit the further resale of the ROXANNE platform and enable centralized software control. Once defined, these measures will be presented in the first version of the project Exploitation Plan.

> *Requirement to ensure that the ROXANNE platform is usable across a diverse range of legal frameworks, note yet possible to evaluate.*
>
> *Requirement to include measures to restrict exploitation to responsible customers, not yet possible to evaluate.*

Article 47 – Right to an effective remedy and a fair trial

This right is defined as:

> *'Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article.*
>
> *Everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law. Everyone shall have the possibility of being advised, defended and represented.*
>
> *Legal aid shall be made available to those who lack sufficient resources in so far as such aid is necessary to ensure effective access to justice.'*

Article 47 of the EU Charter of Fundamental Rights embodies the EU legal principle that Member States must ensure effective judicial protection of an individual's rights arising from Union law (including Charter rights). This means that the right of access to a court applies whenever rights and freedoms guaranteed by EU law are

[264] New Zealand claims world first in setting standards for government use of algorithms, The Guardian, 27 July 2020, https://www.theguardian.com/world/2020/jul/28/new-zealand-claims-world-first-in-setting-standards-for-government-use-of-algorithms ; The ethics of artificial intelligence: Issues and initiatives, European Parliament, Study, March 2020, pp. 66-84 https://www.europarl.europa.eu/RegData/etudes/STUD/2020/634452/EPRS_STU(2020)634452_EN.pdf; Jobin, A., Ienca, M. & Vayena, E. The global landscape of AI ethics guidelines. Nature Machine Intelligence 1, 389–399 (2019). https://doi.org/10.1038/s42256-019-0088-2

involved. It is for EU Member States to establish a system of legal remedies and procedures that ensure respect for rights under EU law.[265]

Access to court is implicit in the right to a fair hearing because it suggests that disputes must be decided by courts. This right is an important element of access to justice given that courts provide protection against unlawful practices and uphold the rule of law. For the right of access to a court to be effective, states may have to provide legal aid, translation or other practical support to enable individuals to access court proceedings.[266]

Relevance and use to the project

Under this project, this right holds much importance with respect to the need for a 'fair trial'. Whether a hearing is considered fair depends on all facts of the case, including the ability of the individual to access justice. The proceedings as a whole (i.e. from the institution of proceedings, including police questioning in criminal cases, to the final determination of an appeal) must be considered.[267] One of the core requirements of the right to a fair hearing is 'equality of arms' between the parties. Equality of arms involves ensuring that each party has a reasonable opportunity to present its case in conditions that do not disadvantage either party. Under EU law, secondary legislation further details the scope of fair trial rights. For example, Directive 2012/13/EU on the right to information in criminal proceedings establishes that suspects and accused persons who are arrested must also be provided with a 'Letter of rights' containing information on additional rights, including their right to access documents relating to their specific case that are in the possession of the competent authorities – such as evidence.[268]

In terms of prosecutions using evidence analysed through the ROXANNE platform, it may so happen that due to lack of complete algorithmic transparency, the results of this platform could not be completely explained or understood by the accused and/or the prosecutor. In such a case, the weighting given to the results of this platform could play a major role in ascertaining whether the trial is fair or not. Also, it might be difficult to share the evidence with the accused if the internal analysis and algorithms form a major component of the result which is deemed evidence against the accused. This could further undermine the 'equality of arms' since the evidence brought forth by an 'opaque' platform cannot be disproven without understanding the internal functioning of it, which itself creates a major disadvantage for the defendant.

As the complexity of data processing/analysis increases, these concerns become more relevant. Whereas, if there is complete algorithmic transparency, it might defeat the purpose of this platform itself. Hence there is a need to ensure a level of algorithmic transparency which is just enough to verify the results of the platform. Further, the court should be well informed about the possible biases/technical constraints which might lead to an incorrect result. The confidence level of the result and understanding of the platform should then empower the court enough to make a fair trial. Then, ensuring fair trial would be a function of competency of the court.

> *Requirement for the data processing operations of ROXANNE to be transparent and understandable to non-technical experts, not yet possible to evaluate.*

[265] CJEU, C-432/05, Unibet (London) Ltd and Unibet (International) Ltd v. Justitiekanslern, 13 March 2007, paras. 37–42.

[266] European Union Agency for Fundamental Rights and Council of Europe, "Handbook on European law relating to access to justice",European Union Agency for Fundamental Rights and Council of Europe, 2016, p.26. Available at: https://www.echr.coe.int/Documents/Handbook_access_justice_ENG.pdf

[267] Edwards v. the United Kingdom, App No 13071/87 (ECtHR,16 December 1992), para 34

[268] European Union Agency for Fundamental Rights and Council of Europe, "Handbook on European law relating to access to justice",European Union Agency for Fundamental Rights and Council of Europe, 2016, 40. Available at: https://www.echr.coe.int/Documents/Handbook_access_justice_ENG.pdf

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

Article 48 – Presumption of innocence and right of defence

This right is defined as:

> *'1. Everyone who has been charged shall be presumed innocent until proved guilty according to law.*
>
> *2. Respect for the rights of the defence of anyone who has been charged shall be guaranteed.'*

This Article is the same as Article 6(2) and (3) of the ECHR. In accordance with Article 52(3), this right has the same meaning and scope as the right guaranteed by the ECHR. This article promises that an individual shall be presumed innocent until proven otherwise.[269] Every person charged with a criminal offence has the following minimum rights:

> *'(a) To be informed promptly, in a language which he understands and in detail, of the nature and cause of the accusation against him;*
>
> *(b) To have adequate time and facilities for the preparation of his defence;*
>
> *(c) To defend himself in person or through legal assistance of his own choosing or, if he has not sufficient means to pay for legal assistance, to be given it free when the interests of justice so require;*
>
> *(d) To examine or have examined witnesses against him and to obtain the attendance and examination of witnesses on his behalf under the same conditions as witnesses against him;*
>
> *(e) To have the free assistance of an interpreter if he cannot understand or speak the language used in court.'*[270]

Relevance and use to the project

The ROXANNE platform (when in use) uses network analysis to track the individuals who might have interacted with a 'suspect'. In such a scenario, the individual who otherwise should be presumed innocent, is being monitored.

Similarly, ROXANNE might implicate someone innocent who might be a close acquaintance of known suspect(s). Such scenarios need to be dealt with carefully and the onus of the same falls on the end-users and courts. It becomes imperative to complement the results of ROXANNE with some other convincing evidence gathered during the investigation. Unless there is this additional evidence supporting the suggestions of ROXANNE platform or unless the result of the ROXANNE can be verified, the defendant should be given the benefit of doubt.

> *Requirement for technical partners to consider the thresholds at which the system highlights items for further investigation in order to given innocent persons the benefit of doubt, not yet possible to evaluate.*

To ensure that no individual is falsely charged based on the results from ROXANNE platform, upon trial every suspect should be made aware of his/her rights specially with regards to Article 47 (Right to an effective remedy and a fair trial), EU Charter of Fundamental Rights. Also, the design and testing of the platform should be influenced by these possibilities and careful attempt should be made to minimise potential cases of 'false-positive' even if it means compromising on the efficacy of the platform to a certain extent.

> *Requirement for false-positives to be minimised in the platform, not yet possible to evaluate.*

[269] Art.6(2), ECHR

[270] Art.6(3), ECHR

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

4.2. T3.3 Scenarios

Scenario 1 – Violent and peaceful protesters

Katy runs a political campaign group that organises protests for better representation of ethnic minorities in public life. She organises a march to support this cause. During the march, a small faction of protesters engages in violence.

In order to identify the violent protesters, LEAs analyse all CCTV of the march using the ROXANNE facial verification tool. This analysis shows that the faction instigated violence at several different sites during the march. The faction is ethnically diverse, but only the violent protesters who are from an ethnic minority are known to the police due to discriminatory policing practices in the past. LEA officers arrest and interview the violent protesters from ethnic minority groups who they have identified.

Question: In order to protect rights of non-discrimination, how should LEAs prevent bias in historical data and historical policing practices from affecting policing activities today?

Answer:

During interviews, violent protesters acknowledge their membership of Katy's campaign group but those in the violent faction refuse to reveal information about other members of the faction. In order to identify faction members, investigators obtain a warrant to examine the communication data of the violent protesters. Investigators analyse the mobile phone data of the offenders using the ROXANNE platform. The results of this analysis reveal other members of the faction and also show that Katy is connected to every offender. Investigators question the violent protesters about whether Katy had any role in instigating violence and conclude that she was not involved.

Question: If the personal data of an innocent person is included in an investigation, how should LEAs balance respecting rights to privacy and the protection of personal data with the needs of an investigation? What factors should be considered?

Answer:

After being released on bail, several of the violent protesters inform Katy that investigators asked questions about her. Katy worries that LEAs will take an interest in her because she organised the march, this leads to high-levels of stress which badly affect her mental health and she passes the leadership of her campaign group to other people.

Question: In order to balance protecting the integrity of the person with needs to protect the public, should LEAs consider the indirect effects that their actions might have on people, particularly if it results in the suffering of those being investigated? Should indirect effects be judged in terms of the proportionality of LEA actions?

Answer:

Following the identification of other members of the violent faction using ROXANNE, they are also arrests. This, combined with the apparent LEAs' interest in Katy, leads peaceful leaders of the campaign group to mistakenly determine that LEAs are trying to deter further peaceful protests. Based on this belief, peaceful

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

campaigners cancel future protests owing to the perceived risks of arbitrary arrest and protesters believing LEA actions to be an attack on their freedoms of expression and assembly.

Question: In order to respect freedoms of expression and assembly and avoid chilling effects, how should LEAs balance the need to communicate their lawful and ethical use of technology in order to build public trust with the need to keep sensitive investigative information and techniques secret so as not to benefit criminal perpetrators?

Answer:

Please use this box to provide any feedback you might have about the scenario as a whole, or any other comments you might have about the implications of ROXANNE for fundamental rights.

Scenario 2 – Extreme writings

Alex is a literature student who is interested in writing about extremist politics. The plot for one of their stories advocates violence in support of an extreme political cause. Alex's university professor is concerned about this and flags the story to the university who report it to a local LEA.

LEA officers assess all information openly available about Alex on the internet, including their social media pages and blog. The LEA analyses this information using the ROXANNE text analysis tools and discovers many mentions of 'guns' and 'bombs', along with many references to killing political enemies.

Question: In order to protect privacy rights, LEA processing of personal data should be restricted to what is lawful, necessary, and proportionate. But, should there be any additional restrictions on LEAs accessing information about suspects that is openly available (e.g. only processing data where citizens would reasonably expect it)?

Answer:

LEA officers are concerned that Alex might be involved in a plot to commit violence and obtain a warrant to intercept Alex's internet traffic to ascertain if this is true. LEAs discover that Alex has been communicating with many political extremists after evaluating their internet traffic. Using network analysis, they show that Alex links several extreme groups across the political spectrum.

Motivated by their growing concerns about Alex's potential plans, investigators present these initial findings to a judge and obtain a warrant for accessing Alex's content data. They discover a large number of Alex's private writings in an online drive; these are analysed using the ROXANNE text analysis tool which shows that Alex has written a manifesto that includes both violent language and plans for attacking specific targets. LEA officers are convinced that Alex is preparing for an act of terrorism and they arrest Alex.

Question: In order to prevent automated decision-making, and to respect rights to liberty and security, how should LEA officers corroborate the results of data-analysis tools before they arrest someone?

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

For example, an investigator could repeat the machine analysis to ensure it is correct, check that key results make sense, or find additional corroborative evidence before acting.

Answer:

Alex's case reaches the trial stage. The prosecution presents the results of analysis done by the ROXANNE platform to show that Alex has been communicating with political extremists, has written extensively on violent political extremism, and has developed specific plans for carrying out violent acts. The defence case argues that Alex is innocent and was communicating with political extremists for a book project that would include samples from a fictional manifesto that includes fake attack plans.

Question: In order to protect the right to a fair trial, should the use of technological results be subject to review by experts before being submitted to court? Should the results be presented in court by experts, as with forensic evidence?

Answer:

The jury are extremely impressed with the technological sophistication of the ROXANNE platform and give the results from the platform greater weight in their discussions than other evidence. They jury convict Alex, although Alex is actually innocent.

Question: In order to protect the presumption of innocence, should safeguards be implemented so that juries can understand, and give a fair assessment of, the results of technological analysis? If so, what safeguards?

Answer:

Please use this box to provide any feedback you might have about the scenario as a whole, or any other comments you might have about the implications of ROXANNE for fundamental rights.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

5. T3.4: Comply with applicable legislation, including in the area of free movement of persons, privacy and protection of personal data

The task description of T3.4 provides the following:

> *'The partners will create digital brochure containing a checklist of the relevant provisions of applicable legislation such as the GDPR, the INTERPOL Rules on the Processing of Data, the Police Directive, the Network and Information Security Directive, etc., how partners and stakeholders can comply with the relevant provisions (update in M36). T3.4 will nominate security advisory board (see Section 6.3.2, Grant Agreement).'*

An explicit mention of the free movement of persons is mentioned in the task title, but not the task description. Upon discussion, the INTERPOL, TRI, and CAPGEMINI determined that it would be best to focus the work of this task of legislation relevant to data processing and data protection, and so legislation about free movement of persons is not discussed here.

In order to develop the checklist, WP3 partners, led by INTERPOL, discussed and decided upon a list of relevant legislation. These are:

- General Data Protection Regulation (GDPR) 2016/679
- Law Enforcement Directive 2016/680
- INTERPOL Rules on the Processing of Data (RPD)
- Council of Europe Convention 108+
- Directive Copyright Digital Single Market 2019/790
- Network and Information Security Directive 2016/114

These different pieces of legislation were then analysed in terms of different provisions which covered:

- Lawfulness of data processing
- Special categories of data
- Data processing principles
- Individual rights
- Accountability &transparency
- Data security
- Data storage & retention
- Data transfer

The pieces of legislation were split between partners[271] and analysed across each of the provisions in order to provide a multi-faceted approach and understanding of different provisions. This analysis was used to create a checklist that partners can use to assess their data-processing during the research and development phase. The text of this is provided below, a reformated version of this has been created and is ready for dissemination. As the checklist provides requirements for partners to abide by, they will not be summarized again here (as with the analysis above) but are provided in the list of requirements in Annex A; so far the partners have complied with the GDPR and so the requirements are being met at this point of the project.

The intention of the partners involved in this task is to create another checklist relevant to the use of ROXANNE that will be included in D3.4 (Final report on compliance with ethical principles), when more is known about the expected use of ROXANNE.

[271] TRI analysed: General Data Protection Regulation (GDPR) 2016/679; Law Enforcement Directive 2016/680. INTEPROL analysed: INTERPOL Rules on the Processing of Data (RPD); Council of Europe Convention 108+; Directive Copyright Digital Single Market 2019/790.
CAPGEMINI analysed: Network and Information Security (NIS) Directive 2016/1148

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

5.1. Checklist document

N°	Legal source	Requirement	Compliance status
1	GDPR[272] Article 6 CoE Convention 108+[273] Article 5	Ensure lawful data processing when developing and testing the ROXANNE platform by relying on a lawful legal basis (i.e. individuals' freely given, specific, informed and unambiguous consent; legitimate basis prescribed by law;performance of a tasks in the public interest; for a legitimate interest that does not override the right and freedoms of the individual).	Individuals' informed consent has been systematically sought for participation in project research activities related to feedback provision (i.e. end-user requirements survey, Field Test evaluations), as well as for collection and preparation of simulated data. When processing research datasets for platform development purposes, partners will invoke the legitimate interest basis.
2	GDPR Article 5 CoE Convention 108+ Articles 4-13 RPD[274] Articles 10-18	Abide by the data protection principles when processing data: • lawfulness, legitimacy, fairness, and transparency; • purpose limitation; • data minimisation; • data quality and accuracy; • storage limitation; • data security, integrity and confidentiality; • transparency, accountability and duties of the parties; • rights of the data subjects;	The project technical team is mindful of these principles and incorporates them in its development activities with legal guidance and support from the project legal team through close dialogue and exchanges. As such, the technical partners safeguard the quality and accuracy of processed data, using only minimal necessary for the performance of a task and completing data protection impact assessment prior to any activity involving high-risk data processing. Further principles are covered in the checklist.
3	GDPR Articles 13-21 CoE Convention 108+ Article 9	Be in a position to satisfy individuals' rights as data-subjects, such as: • to obtain information about, and access to, their personal data that is being processed in an accessible format, at reasonable intervals and without excessive delay or expense; • to rectify or erase inaccurate, false, or unlawfully processed data; • to restrict the processing of their personal data; • to a remedy in case any of the rights are not respected.	The project team has been providing individuals that consented to partake in research activities the contact details of data processors to enable them to exercise their rights as data subject rights, i.e. information sheets given to survey respondents or Field Test participants. For future processing of publicly available data that would entail disproportionate efforts to notify potential data subjects, the Privacy Policy, https://www.roxanne-euproject.org/privacy-policy, posted on the ROXANNE website will cover this aspect of project data processing.
4	GDPR	Satisfy the more stringent requirements	The project counts on the processing of

[272] GDPR

[273] Council of Europe Convention for the protection of individuals with regard to the processing of personal data https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1

[274] INTERPOL Rules on the Processing of Data https://www.interpol.int/Who-we-are/Legal-framework/Data-protection

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

	Articles 9-10 CoE Convention 108 Article 6	applicable when processing special categories of data including racial or ethnic origin data, the processing of genetic data or biometric data for the purpose of uniquely identifying a natural person or personal data related to criminal convictions and offences that can only be processed where it is allowed under Union or national law.	special categories of data, especially biometric data, as part of the development and testing of the ROXANNE platform that aims to unmask members of organized criminal groups. This processing is either based on individuals consent or is performed on data taken from public sources, which is in line with the legitimate interest as a legal basis and scientific research as a condition for processing special category data . The consortium is exploring the possibility of processing personal data related to criminal convictions provided this would be in accordance with the concerned partner's domestic law.
5	GDPR Articles 9-10 CoE Convention N°108+ Article 8, 11, 15	Engage in transparent and accountable data processing, which would enable the consortium to demonstrate compliant data processing and allow data subjects to fully exercise their rights.	The consortium has been informing research participants of the terms and conditions of their data processing through the provision of information sheets, covering both transparency and fairness aspects. The project Privacy Policy details the circumstances of data processing activities when the option of providing each individual with information is not feasible. The consortium operates on a traceable and secure access to project documentation and files stored on the SWITCH cloud with access restricted on a need-to-know basis.
6	GDPR Articles 32-34 CoE Convention 108+ Article 6	Ensure appropriate data security measures are in place.	All of the project partners have specific technical and organizational security measures in place to ensure the integrity, security and confidentiality of project data is maintained. The consortium operates with the minimal data necessary, and whenever possible uses anonymised or pseudonymised data. A project Security Advisory Board, chaired by the project security officer, maintains project security reports and ensures compliance with security rules and respect of the confidentiality level of all deliverables.
7	GDPR Article 5 CoE Convention 108+ Article 5	Time-limited storage of personal data followed by data deletion once purpose fulfilled	The consortium applies specific data retention timeframes depending on the purpose sought, in any case not exceeding 5 years beyond the project termination. Only fully anonymised data may be stored beyond this period.

8	GDPR Articles 45-47, 49 CoE Convention 108 Article 14 RPD Art 62-63	Ensure appropriate protection of individuals with regard to the transborder processing of personal data	The consortium comprises of two partners outside the EU, Switzerland and Israel, both covered by EU adequacy decisions. INTERPOL, as an International Organization has its own data protection framework (INTERPOL Rules on the Processing of Data[275]) offering robust standards for data protection. In addition, respondents to its international survey consented to the data transfers.
9	Copyright in the Digital Single Market[276] Article 3	Comply with the digital single market copyright and related rights provision	The consortium intends to collect open source data, in accordance with the terms and conditions of the selected website. Project partners who are research organizations may take advantage of the text and data mining exception as an important research tool to web-crawl lawfully accessed pages for scientific research purposes.

5.2. Security Advisory Board

This task also involved the nomination and managing of the project's Security Advisory Board (SAB). The purpose of this board is to discuss key security issues, such as data integrity, data confidentiality, and data security. They are also able to review any deliverables flagged to them by partners where there is a potential risk of sensitive information being included in public deliverables. The Board can then advise on changing the classification of the deliverable, or providing an edited version to the public with the sensitive details removed. So far, partners have not flagged potential risks of sensitive details leaking out from the project to the public and so the board does not need to meet regularly. Its members are, however, ready to meet when needed.

This Board was led by Farhan Sahito as project security officer until his departure from CAPGEMINI, the project is currently in the process of appointing a new project security officer. The project will appoint a new project security officer soon.

The members of the Board are:

- Stéphan Brunessaux, Airbus
- Francesco Calderoni, UCSC
- Sébastien Marcel, Idiap
- Damir Osterman, Ministry of Interior Croatia
- Yosef Solewicz, MOPS Israel
- Claudia Ceveninni, University of Bologna (External member, also sits of the External Ethics Board)

[275] INTERPOL Rules on the Processing of Data https://www.interpol.int/Who-we-are/Legal-framework/Data-protection

[276] EU Directive on Copyright in the Digital Single Market 2019/790 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019L0790

6. Overarching and emerging themes

Several issues have been discussed across ethics, societal values, and law. For example, the notion of trust is present throughout each area, in terms of whether end-users will be able to trust the outputs of the platform and whether citizens will be able to trust that the platform will be employed in an ethical and lawful way. In order to build trust, this requires transparency in relation to what processing will take place with the ROXANNE platform, and how. Yet, in terms of citizens, it is possible that this could have the opposite effect. By making it known that LEAs have the significant capabilities afforded by ROXANNE, this could, potentially, result in citizens being concerned about growing abilities that LEAs have and could result in 'chilling effects' where people choose not to engage in innocent behaviours for fear of being subject to analysis by investigators using the ROXANNE platform. Of course, both needs for transparency and avoidance of chilling effects are aims to pursue for the consortium, and so further work on how this tension can be managed should take place in future.

With regard to chilling effects, the potential for ROXANNE to increase chilling effects due to combining of recognition and network analysis technologies and the potential for people's actions to be 'chilled' for both themselves and their acquaintances has been noted several times. This issue should be further explored, particularly in terms of the tension noted above and how the project should disseminate information on the benefits of the ROXANNE platform for investigations alongside details of oversight an accountability mechanisms that should ensure the lawful use of the platform.

Another thread running throughout the document (sometimes implicitly) is the need for requirements to be functional so that technical partners can build the platform to enable end-users to fulfil requirements related to use of the platform. The work of WP3 has centred around an ethics-by-design and privacy-by-design approach to ensure that the project itself is abiding by applicable standards. This enables end-users to be confident that they are using technologies that were responsibly developed. A more material effect is that, through responsible innovation, the ROXANNE platform is less likely to generate issues in future; for example, partners in ROXANNE are taking steps to avoid biased algorithms, this should mean that there should also be less realisation of the effects of bias during use of the platform than if a similar platform were created without addressing this issue.

Linked to this issue is how results should be interpreted. The project partners are clear that the technologies being developed for network analysis can only highlight data points that are unusual in comparison to others, the meaning of this is a matter for investigators to decide using all available information and their knowledge about the context and facts of the case. This reinforces the point that the ROXANNE platform is not intended to replace any human decision-making, it is an assistance tool for helping investigators to deal with analysing data. The partners should, therefore, engage in work to ensure that the human-centred approach avoids risks of automation bias and dehumanisation, as mentioned above (partners are in the early stages of working on how the human-machine relationship should be structured). The presence of human beings is also key to ensuring that the platform is used according to ethical and legal standards, and that someone can be held responsible if it is used in violation of those standards.

Connected to the needs for abiding by legal and ethical standards, is the need to ensure that only responsible customers gain access to ROXANNE. The consortium does not want, and seeks to avoid, exploitation to countries and organisations that will use the ROXANNE tools for repressive means in violation of legal and ethical standards. The partners have already dedicated efforts to developing exploitation guidelines to avoid sales to non-democratic states and those with poor records of complying with human-risks (see D10.16 Report on the risks of misuse and mass surveillance), and partners should continue to refine these guidelines in future exploitation plans.

Dissemination of the work in this document is a recurring topic. Owing to the close inter-working of TRI, CAPGEMINI, and INTERPOL, the work carried out is going to be disseminated together. As explained above, these partners plan to present a webinar to cover ethical, societal, fundamental rights, and applicable legislation issues. This will be partnered with a dissemination package, including the societal values briefing paper, fundamental rights summary paper, and the brochure about applicable legislation. In order to gather feedback, from citizens (as detailed in the T3.2 task description), recipients will be encouraged to fill out a survey, and

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

comment on the scenarios above, following the webinar and reading of the documents in order to provide comment and suggestions about our work. We will then incorporate feedback into our work going forward and adapt it as necessary.

7. Next steps and future work

Following the development of the requirements above, WP3 partners will summarise and present them to partners in order that they are aware of them and can implement them. WP3 partners will then work alongside other partners to ensure the requirements are fulfilled. The requirements will also be discussed with external stakeholders (at the ethics, societal values, and legal webinar, for example), in order that they can be further refined and externally validated.

The work of WP3 then continues in T3.5 by looking at INTERPOL's global communications network to determine how it could benefit deployment of the ROXANNE platform; this will be provided in D3.3 (INTERPOL Global Communications infrastructure). In addition, T3.6 involves the designing of an electronic decision-making mechanism, this will involve converting many of the requirements above into a process that should enable respondents to fulfil those requirements and abide by the applicable standards; this will be provided in D3.2 (Development of a decision-making mechanism).

Further, WP3 partners will continue the work of analysing the project and platform from an ethical, societal, and legal perspective, and monitor the implementation of the requirements suggested above into the solutions of the project. This will take place as part of T3.7, and be provided in D3.4 (Final report on compliance with ethical principles).

8. Conclusion

Overall, this document provides an initial provision of requirements for compliance with ethical, societal, fundamental rights, and applicable legislation standards; it also provides a first assessment of how the project is complying with these standards so far. Through applying these requirements to the work done so far, it can be seen that, at this stage, the ROXANNE consortium is pursuing its research goals according to the standards of ethics, societal values, fundamental rights, and applicable legislation. To ensure that this continues, WP3 partners will assist other partners in the implementation of the requirements provided above to ensure that requirements are met going forward. The results of this implementation will be assessed over the course of the rest of the project, and provided in the next iteration of this deliverable.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

9. Annex B: Tables of requirements

Ethics Requirements	
Phase 1: Requirement Gathering	
Human agency, liberty, and dignity	Requirement to treat survey respondents with respect for their agency, liberty, and dignity completed.
Technical robustness and safety	Requirement to use safe and secure infrastructure to process requirement surveys responses completed.
	Requirement for the requirement surveys to be accurate, reliable, and precise completed.
Privacy and data governance	Requirement for requirement gathering to respect privacy completed.
	Requirement for requirement gathering surveys to ensure relevant, accurate, complete, and reliable data as far as possible completed.
	Requirement to respect the privacy of survey respondents completed.
	Requirement to fulfil data rights and data ownership of data-subjects on track to be completed.
Transparency	Requirement to be transparent about how personal data will be processes completed.
Diversity, non-discrimination and fairness	Requirement to not discriminate against participants, and to treat responses fairly, completed.
Individual, societal and environmental wellbeing	Requirement to respect individual and societal wellbeing during requirement gathering completed.
	Requirement for survey to not use excessive resources completed.
Accountability	Requirement to openly justify decisions based upon the requirement gathering survey not yet possible to evaluate.
Phase 2: Planning and Designing	
Human agency, liberty, and dignity	Requirement to treat consortium colleagues respectfully fulfilled up to this point in the project.
Technical robustness and safety	Requirement for planning and designing to be technically robust and safe completed.
Privacy and data governance	Requirement to respect privacy of consortium partners and consortium confidential documents fulfilled so far.
Transparency	Requirement to be open about decisions regarding data-processing in the project completed so far.
	Requirement to be transparent with the public about the ROXANNE project and its progress expected to be completed.
	Requirement for technical partners to implement measures to ensure data processing by the ROXANNE platform is transparent and understandable to human beings, not yet possible to evaluate.
Diversity, non-discrimination and fairness	Requirement for professional diversity in ROXANNE colleagues completed.
	Requirement for diverse inputs in validating the ROXANNE platform, completed so far.
	Requirement to have a diverse group from which to gather feedback from

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

	completed.
	Recommendation that project partners develop diversity policies if they do not have them, not yet evaluated.
Individual, societal and environmental wellbeing	Requirement to respect individual and societal wellbeing during planning and designing, completed.
	Requirement to not travel excessively for face-to-face meetings, completed so far.
Accountability	Requirement to implement accountability structures completed.
	Requirement to hold partners to account for the quality of their work completed so far.
Phase 3: Development	
Human agency, liberty, and dignity	Requirement to treat human participants involved in data collection respectfully completed so far.
	Requirement to only re-purpose datasets that were created subject to a research ethics framework fulfilled up to this point in the project.
	Requirement for technical partners to check that data to be re-purposed was gathered ethically, to be completed.
	Requirement to use data in ways that data-subjects would expect completed so far.
	Requirement not to create problematic effects for data-subjects completed so far.
Technical robustness and safety	Requirement for platform development to be accurate, reliable, and precise not yet possible to evaluate.
	Requirement for code development to be safe and secure completed.
Privacy and data governance	Requirement not to re-identify data-subjects in pseudonymised or supposedly-anonymised data, completed so far.
	Requirement to respect the privacy of data-subjects when re-purposing data generally fulfilled so far. Fulfilled where data-subjects consented to re-purposing, minor and benign infringement on privacy where data is gathered from the public sphere.
	Requirement to justify any use of LEA use of data from real closed cases, completed with so far.
	Requirement for any LEA use of data from real closed cases to be restricted to benign infringements on privacy, expected to be completed.
	Requirement for any discoveries relevant to illegal activity from data-processing activities reported in accordance with the incidental findings policy, not yet possible to evaluate.
Transparency	Requirement to disseminate non-confidential results, to be completed.
	Requirement to be open with regulatory and oversight bodies, not yet possible to evaluate.
	Requirement to maintain accurate records of data-processing and ethical decision-making, to be completed.
	Requirement to provide the public with an understanding of how the ROXANNE tools work, to be evaluated
	Requirement for technical partners to build the platform to enable LEAs to be transparent by making the algorithmic decision-making explainable so that results can be audited and challenged by supervisory authorities, not yet possible to evaluate.
Diversity, non-	Requirement for ROXANNE to be developed using datasets that represent diverse

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

discrimination and fairness	populations in terms of language, accent, socio-economic background, age, and gender, not yet possible to evaluate.
Individual, societal and environmental wellbeing	Requirement for partners not to put colleagues under excessive work pressures completed so far.
	Requirement for development of the ROXANNE platform to be compliant with societal values, not yet possible to evaluate.
	Requirement for technical partners to give regard to energy efficiency when developing the platform and to endeavour to build a platform that does not consume disproportionate amounts of energy, not yet possible to evaluate.
Accountability	Requirement to integrate legal and ethical considerations into the development of the ROXANNE platform, not yet possible to evaluate.
	Requirement for project partners to be subject to legal and ethical accountability measures completed.
	Requirement for technical partners to develop the ROXANNE platform with technical means (e.g. logging mechanisms) to evidence compliance with accountability measures, not yet possible to evaluate.
Phase 4: Testing	
Human agency, liberty, and dignity	Requirement to treat participants testing the ROXANNE platform with respect not yet possible to evaluate.
Technical robustness and safety	Requirement to assess the accuracy, reliability, and precision of the ROXANNE platform not yet possible to evaluate.
Privacy and data governance	Requirement not to use the ROXANNE platform on ongoing LEA cases completed.
	Requirement to only process closed cases with appropriate approval, completed so far.
	Requirement for LEAs to ensure that any data from real closed cases made available to the project was lawfully gathered, completed so far.
	Requirement for LEAs to assess the privacy implications for data-subjects included in their testing data-sets, completed so far.
	Requirement for any LEA use of data from real closed cases to be restricted to benign infringements on privacy, expected to be completed.
	Requirement to justify any use of LEA use of data from real closed cases, completed so far.
	Requirement for any discoveries of illegal activity during data-processing to be reported in accordance with the incidental findings policy, not yet possible to evaluate.
	Requirement for LEAs to assess the diversity of their testing datasets where practicable, completed so far.
	Requirement for use of LEA data in the ROXANNE project to be regulated under the GDPR, or under strictly limited circumstances if the LED is applicable, completed so far.
	Requirement for LEA data from real closed cases to remain with LEAs, completed so far.
Transparency	Requirement for partners to publicly disseminate results of field-tests, set to be completed.
	Requirement for technical partners to build the platform in such a way to be understandable to persons testing the platform.
Diversity, non-discrimination	Requirement for technical partners to evaluate algorithm for bias and take steps to reduce this, not yet possible to evaluate.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

and fairness	Requirement for test datasets to be varied and representative, not yet possible to evaluate.
Individual, societal and environmental wellbeing	Requirement for training provision to make clear that the ROXANNE platform is a machine and should not be anthropomorphised, not yet possible to evaluate.
	Requirement for exploitation of the platform to not anthropomorphise it, not yet possible to evaluate.
	Recommendation for exploitation partners to consider changing the name of the platform to a non-human name, not yet possible to evaluate.
	Requirement for partners to only send necessary persons to field-tests and meetings, not yet possible to evaluate.
Accountability	Requirement for test data choices to be discussed amongst the consortium and potentially wider stakeholder group, not yet possible to evaluate.
	Requirement for any technical partners accessing LEA data to log the circumstances of this, not yet possible to evaluate.
Phase 5: Evaluation	
Human agency, liberty, and dignity	Requirements for participants to be able to give feedback and for responses to be treated fairly and equally not yet possible to evaluate.
Technical robustness and safety	Requirement for technical work to be widely reviewed within the consortium and to ensure components fulfil LEA needs not yet possible to evaluate.
Privacy and data governance	Requirement to plan interviews according to applicable standards of research ethics not yet possible to evaluate.
	Requirement for interviewees to not be pressured and treated according to research ethics standards not yet possible to evaluate.
	Requirement for interview questions to enable data gathering that is relevant, accurate, complete, and reliable not yet possible to evaluate.
	Requirement to give data-subjects interviewed during the evaluation phase ownership over their data not yet possible to evaluate.
Transparency	Requirement for partners to be transparent about shortcomings of the platform during evaluation not yet possible to evaluate.
	Recommendation for the project partners to add a summary of ethical and legal concerns and solutions to the project website not yet possible to evaluate.
	Requirement for technical partners to build the data-processing modules and overall platform in such a way that it can be understood and evaluated.
	Requirement for technical partners to build the ROXANNE platform so that it is understandable to LEAs.
Diversity, non-discrimination and fairness	Requirement for partners to treat results and feedback equally, impartially, and openly not yet possible to evaluate.
	Requirement to build the platform to take into account different needs of potential users not yet possible to evaluate.
Individual, societal and environmental wellbeing	Requirement to respect individual, societal, and environmental wellbeing during the evaluation phase, set to be completed.
Accountability	Requirement for the project partners to take responsibility for production of a platform in line with that agreed in the Grant Agreement.
Phase 6: Use	
Human agency,	Requirement for technical partners to build the ROXANNE platform in such a

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

liberty, and dignity	way as to require LEA officers to make all decisions, not yet possible to evaluate.
	Requirement for training materials to highlight that the LEA users should treat the ROXANNE platform as an assistive tool, not yet possible to evaluate.
	Requirement for promotion and exploitation of the platform to avoid implications that the platform can automate decision-making, not yet possible to evaluate.
	Requirement for ROXANNE researchers to try and understand the informal professional needs not yet completed.
	Requirement for partners to ensure the ROXANNE platform is developed according to applicable legal standards, not yet possible to evaluate.
	Requirement for partner to avoid exploitation to customers who pose a risk of engaging in unlawful activity, not yet possible to evaluate.
	Requirement for ROXANNE not to be exploited to LEAs with a poor track-record of complying with human rights law, not yet possible to evaluate.
Technical robustness and safety	Recommendation for LEAS to only use the ROXANNE platform on secure systems.
	Recommendation for LEAs to critically evaluate platform outputs in terms of their accuracy, reliability, and precision prior to acting on them.
	Recommendation for LEAs to not treat ROXANNE outputs as conclusive, or indicative of criminality.
	Requirement for partners to make potential customers aware of the context in which the models were built, and how this affects the outputs of the platform not yet possible to evaluate.
	Requirement for the ROXANNE training provision to include information about the meaning of ROXANNE outputs not yet possible to evaluate.
Privacy and data governance	Requirement for technical partners to determine a minimum level of data quality that the platform can reliably be used to analyse, not yet possible to evaluate.
	Recommendation for LEA officers to be cognisant of the limited utility and potential for erroneous outputs when using poor quality data.
	Recommendation for LEA investigators to generally restrict access to data to the investigation team, and only allow access to other investigators for legitimate reasons.
	Requirement for technical partners to incorporate mechanism for logging uses of the ROXANNE platform not yet possible to evaluate.
	Recommendation for LEA officers to log their uses of the ROXANNE platform, and the reasons why.
	Recommendation for uses of the ROXANNE platform to be evaluated by persons independent from investigations.
	Recommendation for sensitive LEA data to remain with LEAs.
Transparency	Recommendation for LEAs to be open about their use of ROXANNE, and supervision of this, as much as possible taking into account operational needs.
	Requirement for the functioning of the ROXANNE platform to be knowable in order that it can be subject to public analysis and accountability measures, where necessary.
	Requirement to gather feedback on potential issues that could be generated by use of the ROXANNE platform, not yet possible to evaluate.
	Requirement for the ROXANNE consortium to explain the intended platform and its uses in publicly available dissemination materials, not yet possible to evaluate.
	Recommendation for LEAs to process data in accordance with the LED.
	Recommendation for LEAs to be open about their policies for processing personal data.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

Diversity, non-discrimination and fairness	Recommendation for LEAs to update training materials to highlight potential discrimination issues present with end-users.
	Requirement for ethics and legal partners to evaluate decision-making mechanism for mitigating discrimination issues, not yet possible to evaluate.
	Requirement for exploitation process to avoid provision of ROXANNE technologies to non-authorised users and authoritarian regimes, and follow the exploitation guidelines, not yet possible to evaluate.
Individual, societal and environmental wellbeing	Requirement for ROXANNE partners to consider the implications for persons finding out that they have been analysed by the platform, not yet possible to evaluate.
	Recommendation for LEA officers to consider the proportionality of using analytical tools in the ROXANNE platform during investigations.
	Requirement for ROXANNE partners to evaluate how data analysis will be presented to end-users so that it complements LEA procedures and assessing proportionality of decisions in investigations, not yet possible to evaluate.
	Requirement for the ROXANNE platform to gather and disseminate wide-ranging views, not yet completed.
	Recommendation for LEAs to engage stakeholders on the procurement and use of ROXANNE, and consider implementation of an ethics board.
	Requirement for technical partners to consider reducing the amount of energy used by ROXANNE, not yet possible to evaluate.
	Recommendation for partners to consider if wasted energy could be re-used, not yet possible to evaluate.
Accountability	Requirement for the ROXANNE platform to have integrated oversight mechanisms and access controls, not yet possible to evaluate.
	Requirement for the training provision to incorporate good practice regarding the ethical responsibilities of end-users, not yet possible to evaluate

Societal Values Requirements	
Citizens' Privacy	Requirement for technical partners to only process personal data according to a sound legal basis, completed so far in the project.
	Requirement for there to be a clear link between the need to process particular data and the design of the platform, completed so far in the project.
	Requirement for the technical partners to incorporate data security by design and by default in the system architecture while ensuring lawful data processing, completed so far in the project.
	Requirement for ROXANNE partners to conduct data protection impact assessments where required, write easy-to-understand privacy policies, provide information about processing to data-subjects, and not make personal data automatically available to the public, completed in the project so far where required.
	Recommendation for LEAs to follow data protection legislation in any use of ROXANNE.
	Recommendation for LEAs to ensure data processed using ROXANNE was lawfully collected.
	Requirement for technical partners to facilitate LEAs attesting to lawful data collection, not yet completed.
	Requirement for exploitation to be limited to responsible LEAs who maintain a good track-record of complying with human rights, not yet possible to evaluate.
Trust and the perception of	Requirement for technical partners to build the ROXANNE platform in such a way that it can be understood, and its processes and decisions can be explained to the public, not yet

safety	completed.
	Recommendation for LEAs to be open with the public about their data-protection policies, including data-retention and how data-subjects can exercise their rights.
	Requirement for technical partners to built the platform in such a ways to enable logging of data-processing activities, not yet completed.
	Recommendation that LEAs consider implementing internal oversight mechanisms to evaluate use of data-processing technologies for operations.
Unintended consequences of technological solutions	Requirement for technical partners to optimise the accuracy of algorithmic outputs, whilst taking risks of false positives and false negatives into account, not yet possible to evaluate.
	Requirement for training provision to include information on the limitations of the platform, and implications of use, not yet possible to evaluate.
Social Acceptability	Recommendation for LEAs to be open about the types of data-processing operations they engage in using ROXANNE.
	Recommendation for LEAs to have strong privacy policies that are publicly available.
	Requirement for technical partners to include information on accuracy and data-security in dissemination activities.
	Requirement for technical partners to take citizens' feedback into account during platform development, not yet possible to evaluate.
	Requirement for ROXANNE partners to highlight data-security measures, the expected impact ROXANNE will have on preventing and fighting crime, how the project is dealing with risks of false negatives and false positives, oversight mechanisms, and legal protections, not yet possible to evaluate.
Democracy and Solidarity	Requirement for ROXANNE partners to avoid exploitation to authoritarian states, not yet possible to evaluate.
	Requirement for ROXANNE partners to implement processes to ensure decision-making processes prevent use of the platform in contravention with ethical and legal standards, not yet possible to evaluate.
	Requirement for training provision to highlight ethical and legal issues, not yet possible to evaluate.
Equality and tolerance	Requirement for technical partners to implement measures to assess and minimise the effects of biased data on ROXANNE tools, or incorporate diversity into training datasets, not yet possible to evaluate.
Human Rights	Requirement for decision-making processes to enable compliance with human rights law by requiring end-users to explain the necessity and proportionality of their data-analysis activities, not yet possible to evaluate.
Respect for Human Life	Requirement for ROXANNE partners to build the platform in such a way as to avoid automation bias and prioritise human decision-making, not yet possible to evaluate.
	Recommendation for LEAs to use ROXANNE as an assistive tool in human-led investigations.
The Rule of Law	Requirement for ethical/legal partners to disseminate information about risks of advanced technologies for court proceedings, not yet possible to evaluate.

Fundamental Rights Requirements	
Article 3 – Right to the integrity of the person	Requirement not to impair the physical integrity of human participants in research completed.
	Requirement not to impair the mental integrity of human participants in research completed.
	Recommendations for LEAs to not impair the physical integrity of surveillance subjects when using the ROXANNE platform.

	Recommendation for LEAs to enact measures to protect the psychological integrity of surveillance subjects if they experience mental suffering following disclosure that they were under surveillance.
Article 4 - Prohibition of torture and inhuman or degrading treatment or punishment	Requirement for partners to avoid causing severe suffering to colleagues completed.
	Recommendation for LEAs not to use the ROXANNE platform to cause severe suffering to individuals.
Article - 6 Right to liberty and security	Requirement to respect people's right to liberty and security likely to be complied with if the project meets high standards of scientific research and its tools and platform are properly tested.
Article 7 - Respect for private and family life	Requirement for LEA officers to ensure any data made available to be used in the project was gathered lawfully, completed so far.
	Requirement to respect the private and family life of data-subjects by considering if other, less-sensitive, data sources that real closed case data are available, completed so far.
	Requirement for technical partners to build the ROXANNE platform in such a way that data is not automatically subject to both recognition and network analysis technologies, not yet possible to evaluate.
	Recommendation for LEAs to only use ROXANNE tools to infringe upon the privacy of persons where it is provided for in domestic law.
	Requirement for technical partners to enable LEAs to attest to their lawful use of data, not yet possible to evaluate.
Article 8 - Protection of personal data	Requirement for the project to comply with data protection legislation likely to be complied with.
	Requirement for technical partners to facilitate end-users demonstrating compliance with data protection legislation prior to use, not yet completed.
Article 11 – Freedom of expression and information	Requirement to respect freedom of expression in the project likely to be completed.
	Recommendation for end-users to respect freedom of expression when using the ROXANNE platform by only using it where necessary.
Article 12 - Freedom of assembly and association	Requirement to respect freedom of assembly within the project complied with.
	Recommendation for end-users to respect freedom of assembly.
Articles 21 to 26 – Rights to non-discrimination	Requirement for technical partners to train and build the ROXANNE tools to avoid discriminatory biases to be evaluated.
	Requirement to treat all feedback on the ROXANNE platform fairly and without discrimination completed so far.
	Requirement to ensure that the ROXANNE platform is usable across a diverse range of legal frameworks, note yet possible to evaluate.
	Requirement to include measures to restrict exploitation to responsible customers, not yet possible to evaluate.
Article 47 – Right to an effective remedy and a fair trial	Requirement for the data processing operations of ROXANNE to be transparent and understandable to non-technical experts, not yet possible to evaluate.
Article 48 – Presumption of innocence and right of defence	Requirement for technical partners to consider the thresholds at which the system highlights items for further investigation in order to given innocent persons the benefit of doubt, not yet possible to evaluate.
	Requirement for false-positives to be minimised in the platform, not yet possible to evaluate.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

Applicable Legislation Requirements	
Selected privacy and data protection provisions applicable during the research and development phase	Requirement to ensure lawful data processing when developing and testing the ROXANNE platform by relying on a lawful legal basis, completed so far.
	Requirement to abide by the data protection principles when processing data, completed so far.
	Requirement to be in a position to satisfy individuals' rights as data-subjects, completed so far.
	Requirement to satisfy applicable Union or national law when processing special categories of data, completed so far.
	Requirement to engage in transparent and accountable data processing, completed so far.
	Requirement to ensure appropriate data security measures are in place, completed so far.
	Requirement for time-limited storage of personal data followed by data deletion once purpose fulfilled, completed so far.
	Requirement to ensure appropriate protection of individuals with regard to the transborder processing of personal data, completed so far.
	Requirement to comply with the digital single market copyright and related rights provision, to be evaluated.

10.Annex A: Ethics Touchpoint Table

ROXANNE: Ethics Touchpoint Table					© Trilateral Research (Joshua Hughes) 2020
	Tasks	Task descriptions	Potential Ethical issues	Addressing these issues	Assessment of risk Low: Minimal likelihood that the risk will materialise. Medium: Some likelihood that the risk will materialise. Appropriate actions (counter-measures) should dispense with the risk. High: The likelihood of the risk materialising is high, but the risk can be avoided or minimised or shared with appropriate countermeasures.
WP1	Management				

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

	T1.1	Establishment of Management Structure	The Management structure proposed for ROXANNE aims at facilitating the cooperation between partners while maintaining a strict control of gradual achievements of the action objectives. Responsibilities are clearly defined in the management structure with well-defined roles as presented in Section 3.2, page 64 of this document (grant agreement). This task will also produce the Project Handbook, a deliverable which will contain the information needed by the partners to proceed on various administrative (but also dissemination/exploitation) aspects of the project.	Balancing project management between people of from difference genders, geographical locations, cultures, and professions. Unequal relationships among members of the consortium may lead to some voices being silenced while other may dominate	Project boards should be diverse in terms of gender, geography, cultural background, and profession. Geographic and cultural diversity should be to the extent reasonably possible within a European-centric context.	Low
	T1.2	Management, internal communication and reporting	The Project Coordinator, in collaboration with the management structure of the project, will assume responsibility for contacting the Project Officer, formulating propositions for possible modifications of the work plan, supervising contacts with all LEA organizations and delivering all types of reports to EC. T1.2 will also ensure the day-to-day project management and internal follow up of the administrative tasks, manage the internal project budget, and monitor the resource usage.	Data governance issues due to the Project Management Committee (PMC)holding substantial amounts of data. Transparency and accountability issues due to authority of the PMC and no complaint/appeal mechanism.	The PMC, comprising WP leaders, will discuss issues confidentially unless partners/stakeholders who are the subject of discussions waive their confidentiality. To provide some transparency, decision-making involves all WP leaders. Decisions are made by agreement and involve any partners who may field aggrieved by a decision.	Low

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

	T1.3	Scientific/Innovation Coordination	The purpose of this task is to remark the importance of innovation coordination, especially with respect to the collaboration with industrial partners. The activities will primarily be to communicate all technical work done by technical partners, thus well prepare the technology to be tested on LEA's side, involving real data. This task will also be responsible for communication among technical and end-user partners for the field-testing preparation (in assistance with KEMEA, NFI and INTERPOL).	Technical robustness and safety issues regarding quality of the product. Fairness, Transparency, Accountability issues regarding how decisions about the product are made.	The PMC, WP, and task leaders will review all innovations for their compliance with technical standards and ethical guidelines.	Low
	T1.4	Quality Assurance and risk management	The quality assurance and risk management will be arranged by the Project Coordinator and the Innovation Coordinator, who will report to the Project Board about any significant deviation, and will define the quality procedures of the project (data experimentation process, access to real-data provided by LEAs) according to suitable standards, including guidelines and procedures. The quality plan will be delivered as an integral part of project reports, but the quality assurance task will work during the entire project to ensure the quality of the project results. This quality plan will be	Technical robustness and safety issues regarding the quality of innovations. Transparency and Accountability issues regarding how the decisions about innovation are made. Individual wellbeing issues in terms of sufficiency of risk management.	The partners are creating a peer-review system for all deliverables. Risk identification, assessment and management will be a standing item on monthly PMC meetings, this will allow all partners to add to discussion and ensure adequate technical robustness, transparency/accountability, and wellbeing of individual colleagues.	Medium

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

			applicable to all project's activities, and strict compliance with it is mandatory for all partners. This task will also take care of effective management of risk across the project (Table 3.2b, Grant Agreement).			
	T1.5	Elaborate the project's data management plan	The partners will develop a Data Management Plan (DMP) for the project. The DMP will outline what data the project will generate, whether and how it will be exploited or made accessible for verification and re-use, and how it will be curated and preserved. The DMP will cover all aspects of data and will be regularly updated.	Data governance issues due to the large amounts of information about different partners being held. Transparency issues regarding exposure of partners data stores and data handling processes to the consortium and EC. Accountability issues regarding how partners may be held accountable for not providing the necessary information, or not abiding by the DMP.	The DMP will exemplify best practice regarding data governance. Partners may highlight any information on their data handling practices which they do not wish to share. Partners may be held to account for their actions under Article 7 of the Grant agreement (also note 'Risk 2' in Section 1.3.5 of the DoA).	Low
WP2	End-user requirements and End-use cases					

	T2.1	Collection of End-User Requirements	Besides NFI and other LEAs, the project will involve a wide group of end-users (stakeholders): LEA experts worldwide, through the INTERPOL's global law enforcement network. In order to collect end-user requirements from these stakeholders, NFI will prepare a global survey, validated by ROXANNE partners. This survey will be communicated through INTERPOL's network (192 member countries) of National Central Bureaus (NCBs) and also completed by members of external Advisory Board (AB) and will be communicated at the end-user meeting organized at 1st field-test (M9). NFI and INTERPOL will create a group of project stakeholders to be invited to attend 2nd (M20) and 3rd field-test (M30) meetings (separate budget reserved through ROXANNE coordinator, see Table 3.4b at page 70). The goal is to collect additional feedback and new knowledge in the project's field. This process will include direct interaction with LEA officials working under operational conditions.	Privacy and Data governance issues regarding personal data in responses to the survey. Diversity, non-discrimination, and fairness issues in terms of selecting members of the Stakeholder Board.	The partners will collect end-user requirements taking into account privacy and data governance standards in particular. We will anonymise individuals, if they are mentioned at all in survey responses. The survey responses will be diverse, due to being distributed through INTERPOL's global communications network. We will ensure a balance of participants in the Stakeholder Board according to gender, geographical, and cultural background.	Low

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

	T2.2	Analysis of End-User Requirements	T2.2 aims to compile and categorise end-user requirements based on the outputs of T2.1. The first field-test (M9) will also discuss and validate the development of end-user requirements. This task will also integrate with WP3. In order to facilitate the implementation of Privacy by Design approach to data protection, a review of existing and new legal and ethical safeguards will also take place (assisted by CAP and TRI).	Privacy and data governance issues from handling survey data. Diversity, non-discrimination and fairness issues in terms of how end-user requirements are chosen. Individual wellbeing issues if some end-user requirement are ignored, particularly those related to disability and access needs.	Partners are aware of good data governance practices and will follow them. The partners will analyse anonymous end-user requirements, so the data will be treated fairly. Partners will give due regard to access needs for those with disabilities.	Low
	T2.3	Use-Case Validation	Three operational use-cases will facilitate the development and testing of the ROXANNE technology. These use-cases will reflect LEA's needs and will be developed in the context of criminal investigations and international police cooperation. The use-cases will provide the consortium a clear understanding of the end-user requirements and priorities for the development of ROXANNE outcomes and will serve as a basis for the implementation of appropriate legal safeguards (WP3) will drive technical developments (WP4-WP7), and prepare the Field Tests (WP8). The consortium will rely on three already elaborated operational use-cases (Section	Diversity, non-discrimination, and fairness issues in terms of whether the use-cases are representative of the populations where ROXANNE will be used. Technical robustness issues regarding the ability of the system to perform the required task. Dignity, Privacy and Data Governance issues if the use-cases include real personal data.	The partners will ensure that use-cases are anonymised so as to not offend human dignity, or include personal data, while taking into account that the purpose of the project is to help LEAs to more quickly identify criminals and suspects. Partners will also ensure that the ROXANNE system is technically robust and safe for using these use-cases.	Low

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

			1.3.1, page 10, Grant Agreement).			
	T2.4	Technology Requirements	This task will identify, collect and analyse technological requirements and will specifically aligned with (a) user requirements for field-tests, (b) hardware and (c) software requirements related to integration (i.e. SW architecture). This task is tightly interrelated with T2.1 and T2.3.	Privacy and data governance issues if personal data is included in survey responses. Technical robustness and safety issues if the technology requirements for each part of the project do not work well together. Transparency and Accountability issues regarding who decides on technical requirements for the final system, and how.	The partners will ensure technology requirements include technical robustness and safety, that they factor in data protection, in a way that is compatible with the purpose of identifying criminals or suspects'. The partners will ensure that how they proceed is made transparent to the project's ethics board. The partners recognise that they are accountable to the EC PO as well as to stakeholders, the stakeholder board, and the ethics board.	Low
	T2.5	User Training Requirements	This task will create and refine engaging curricula tailored for each of the targeted end-user categories defining both the theoretical and practical training that will occur through e-learning, or physically at workshops aligned with field-test meetings. These curricula aim to heighten end-user awareness about technical, security and operational aspects. User training requirements will be acquired through interviews, or online surveys (i.e. part of T2.1). Then, based on the previous responses, specific user-groups will be defined and the relevant	Privacy and data protection issues if personal data is included in survey responses. Diversity, non-discrimination, fairness, and individual wellbeing issues if training materials are not appropriate for a wide range of possible users, including those with access needs.	The partners will ensure users' data is securely protected, that they select a diverse group of users for training and that such training is appropriate for all persons involve	Low

			learning process inside the online training platform will be designed. The adapted learning process will entail both theoretical and practical educational material (presentations, video, simulations, other documentation), ranked in specific levels of difficulty.			
WP3	Compliance with EU Societal Values, Fundamental Rights and legislation					
	T3.1	Adhere to Good Ethical Practices				
	ST3.1. 1	Logistics	TRI will establish an ethics board (see section 3.2, Grant Agreement). The partners will compile a list of the titles and contact details of the national ethics committees in the countries of the partners or the partner institution's own ethics committee. In other instances, TRI will form a project ethics board. The partners will prepare informed consent for use in interviews and workshops. TRI will ensure that partners obtain and keep on file the opinions or approvals by ethics committees and/or competent authorities.	Fairness issues in terms of how ethics board is chosen. Transparency issues in terms of how the decisions of the Ethics Board are made and disseminated. Accountability issues in terms of how the Ethics Board can be held accountable for their decisions.	The Ethic Board was chosen to reflect a balance in terms of gender, background, and previous experience with the project. The members of the Ethics Board are using various standard ethics tools/frameworks to address the issues, which will also be available to Partners. The decisions of the Ethics Board are included in reports which are deliverables that are viewable by all members of the consortium and the EC.	Low

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

	ST3.1.2		Identify and assess ethical issues arising from the project: The partners will compile a list of all the activities to be undertaken and will identify and assess any ethical issues that might arise from each of those. The partners will discuss with the WP leader what measures could be taken to address the ethical issues proposing solutions and future steps.	Transparency and Accountability issues as the ethical issues are being assessed by a small team without minutes. Diversity issues as the team are all of a similar background.	The ethical issues highlighted in this task will be assessed by the Ethics Board, thereby providing transparency and accountability through interrogating the work and its methods of production. Diversity issues are mitigated through a diverse Ethics Board providing comments and suggestions on the ethical analysis.	Low
	T3.2	Comply with Societal Values	CAP and TRI will conduct a literature review on societal values and draft a workshop briefing paper. A workshop with external AB members will be convened (i.e. end-user workshop organized at KEMEA in M9) to discuss (a) how the project will address societal values and (b) what measures can be taken to avoid any harm to societal values. The partners will create a series of brief scenarios (vignettes) featuring different societal values (as the perception of security, possible side effects of technological solutions and societal resilience) and how the project will address them, post them on the project website and invite reactions from citizens.	Human Agency, Dignity, Fairness, and Individual well-being issues in terms of how workshop participants are treated, and their opinions are valued. Diversity issues regarding who is invited to the workshop.	Partners will follow standard ethical guidelines in how to treat human participants in the workshop. Their feedback will be anonymised in order that their submissions are treated fairly. Participants will be invited from ROXANNE partners, and the Stakeholder list, and so the diversity of the workshop will, somewhat reflect the Euro-centric consortium.	Medium
	T3.3	Comply with Fundamental Rights	The partners will prepare an analysis about what and how	Diversity issues as the EU Charter on Fundamental	Partners will endeavour to include comparative	Low

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

			fundamental rights might be impacted by the project's proposed solutions. The partners' analysis will be based on selected rights from the Charter of Fundamental Rights of EU. The analysis will provide several examples, like the vignettes in the previous task. The partners will disseminate the analysis to LEAs exploiting INTERPOL's global LEA network, policymakers, and civil society organizations.	Rights is inherently Euro-centric. Privacy and data governance issues regarding dissemination of the analysis. Human dignity issues in terms of how the needs and rights of human beings are assessed.	perspectives of fundamental/human rights as far as they are applicable. Partners will follow good data governance standards when disseminating the research. Partners will consider the implications and effects of the ROXANNE project and platform whilst respecting the individual humanity of all colleagues/end-users.	
	T3.4	Comply with Applicable Legislation	The partners will create digital brochure containing a checklist of the relevant provisions of applicable legislation such as the GDPR, the INTERPOL Rules on the Processing of Data, the Police Directive, the Network and Information Security Directive, etc., how partners and stakeholders can comply with the relevant provisions (update in M36). T3.4 will nominate security advisory board (see Section 6.3.2, Grant Agreement).	Human agency and dignity issues through the partners themselves not deciding upon what legislation is relevant to their work. Privacy and data protection issues through developing contacts for the advisory board.	Colleagues will decide upon the relevance and applicability of legislation with regard for the dignity and agency of partners. Their choices will be screened via the Ethics Board to ensure that risks are as low as practicable in the circumstances of developing standard ethics protocols/codes for partners to abide by. Partners will abide by good data governance practices when nominating members of the Security Advisory Board.	Medium

	T3.5	Examine the potential of Using INTERPOL's Global Comms Network	INTERPOL will explore the possibility of using its global communications infrastructure and data storage mechanisms to facilitate the speedy exchange of data.	Privacy and data governance issues with INTERPOL processing large amounts of personal contact data. Technical robustness and safety issues regarding the security of INTERPOL's global communication system.	The communication activities of INTERPOL are carried out in accordance with INTERPOL's Rules on the Processing of Data, which incorporate set a high level for data protection. INTERPOL's Global Communication Network has been demonstrated to be secure over several years.	Low
	T3.6	Develop a Decision-Making Mechanism	The partners will create a framework, based on the forgoing tasks that will help stakeholders determine whether they comply with ethical principles, social values, fundamental rights and relevant legislation. The partners will send the decision-making mechanism to Data Protection Officer organisations in project member countries.	Human agency and dignity issues regarding the partners themselves not being able to decide what issues are relevant to them, and how they should be dealt with. Technical robustness issues in terms of whether the decision-making framework will be useful in the real world. Transparency and Accountability issues regarding how the decision-making framework is constructed and what assumptions are inherent to it.	What exactly the decision-making mechanism will look like is yet to be determined. But the partners will ensure it is technically robust and transparent through subjecting it to review by other partners. Its decisions will be made accountable through including the name and details of the developer(s) who will be available throughout the project for consultation on how the framework should be used.	Medium

	T3.7	Validate How Best to Integrate Considerations of Ethics, Fundamental Rights, and Social Values into the Project's Proposed Solutions	Bringing together key stakeholders, both internal and external, the partners will discuss the framework, and decision-making mechanism on how considerations of societal values, fundamental rights and applicable legislation can be effectively integrated into the project’s solutions. TRI will interact with other WP leaders on a monthly basis, to ensure that PbD and PIA considerations (both introduced in pages 18 and 18 in Section 1.3.6, Grant Agreement) and ethics considerations are built into technical solutions.	Technical robustness issues regarding the efficacy of the Privacy by Design and how it will work in the ROXANNE system. Privacy and Data governance issues in terms of holding contact data of the stakeholders.	Solutions to technical robustness issues cannot yet be proposed as the partners have yet to determine exactly how best to integrate societal and other ethical values into the project’s solutions, but suffice it to say that the partners will test all proposed solutions in terms of their social considerations and compliance with legislation. Privacy and data governance issues can be resolved through following good data governance procedures.	Medium
WP4	Data management					

	T4.1	Inventory of Analysis of Lawfully Intercepted Data	This task will involve all LEA partners, and will consider all legal and ethical aspects which will arise w.r.t. using real (sensitive) data in the project. It will also prepare a list of data and their potential use in the project according to the classified sensitivity levels: (1) data for project R&D activities available only on secured LEA premises; (2) data for project R&D activities which can be accessed through either a secured collaborative platform, or through access to the ROXANNE remote platform on KEMEA premises; (3) data for project R&D activities with significantly less constraints on their use within the project (specifically targeted in T4.3). The task activities will be in detail supervised by the ethics board and security advisory board (see page 66, Grant Agreement).	Dignity and privacy issues raised by using real data from criminal cases. Data governance issues raised by providing access to different forms of the data. Transparency issues in terms of why data was chosen/made available. Accountability issues regarding who has access to this data.	Partners will anonymise real data as far as is practicable, and pseudonymise other data as far as practicable to mitigate dignity and privacy issues; some indignity might remain but this would be unavoidable in order to make the tests as real as possible. Partners will follow good data governance practices, including noting those who have access to the data. The reasons for choosing a particular group of data will be made clear to the users and the project partners.	High

	T4.2	Overview of Publicly Available Data	This task will provide a survey of existing publicly available resources, mitigating the unavailability of LEA data for technology development. Focus will be on: (i) Commercial databases as the ones available from Linguistic Data Consortium (LDC). (ii) Multimedia data from which relations can be inferred and where a significant amount of meta-information is available. (iii) Publicly available data - YouTube, Vimeo, etc., allowing tests of the developed approaches on data that was not used in training. Publicly available data might as well complement the investigation data (T4.1).	Technical robustness issues as the commonly available data sets may not be particularly useful for the ROXANNE system. Diversity issues if the data sets are not curated in a way which recognises gender and minority differences. Individual and societal issues if ROXANNE is trained on a dataset that is not fair or diverse.	Partners will ensure that the data sets used for building ROXANNE are sufficiently robust for use. Partners will also assess the commonly available data sets to ensure they are including data from diverse populations.	Medium
	T4.3	Social Media Data Ingestion	This task comprises the connection to social media platforms identified as being relevant by end-users through WP2, especially to the data resources identified in T4.1 and T4.3. Modalities will include text, video, audio and multimedia as well as any legally available associated metadata. The resulting components and framework will be structured such as to allow the swift addition of further platforms. This task will also consider including the forum of the INTERPOL's International Child Sexual Exploitation (ICSE)	Privacy, data governance, transparency, and dignity issues of using social media data of individuals who did not anticipate their data being used in this way.	Partners will anonymise social media data as far as is practicable, and pseudonymise other data in order to mitigate the privacy and data governance issues. Transparency issues would be alleviated where pseudonymised data is still personal data (due to the inclusion of identifying additional information), and the individuals can be asked to consent to their data being used. Some dignity issues would remain as the data	Medium

			database, accessed via the I-24/7 network. This will allow connected LEAs to use the hash set of the available image/video material from ICSE for the use in the ROXANNE platform (relation analysis).		comes from real people.	
	T4.4	Data Pre-Processing for Development and Demonstration	The data from different sources (lawful interceptions, open sources, etc.) comes in a multitude of encodings and formats. The first aim of this task is to suggest common data interchange formats. We will consider both legal and technical means to protect information needed for T4.6 and T4.7. The data is also most likely to vary in terms of quality (noisy audio recordings, non-standard characters, blurred images or interruptions in geo-location signals). We will also employ the data cleaning and enhancement methods.	Dignity issues related to people being reduced to data points. Privacy and data governance issues related to colleagues accessing this data. Transparency and accountability issues related to how decisions about the data are made.	Privacy and data governance issues can be mitigated through good data governance practices. Transparency and accountability issues can be mitigated through partners being open about their decisions and providing their reasoning to colleagues in their deliverables. Dignity issues will still remain as the data is always from a real person.	Medium

	T4.5	Case Management	ROXANNE case management component will be implemented to facilitate efficient collaboration within the consortium and make project outcomes suitable for international police cooperation. Main responsibilities are storage and retrieval of data (raw and processed) to ROXANNE internal components. This will enable following features for the end user: evidence tracking, storage of results, data export, activity tracking, as well as the automated case queries and case-specific notifications.	Data governance in terms of how data is stored and accessed. Privacy and accountability issues related to who can access personal data of data subject(s) and why.	Partners will follow good data governance practices. Partners will also ensure that colleagues are aware of what grounds they must have for accessing data through the ROXANNE platform; ideally all occasions of accessing data through the platform will be logged.	Medium
	T4.6	Target Data Simulation for Development and Demonstration	This task deals with the definition of scenario, amounts of data, channels (telephone, Skype, etc.), relevant metadata and with the actual recording. We will collect a limited amount of audio-textual-video data simulating the behavior of a criminal network, within the consortium in two selected target languages, and on real LEA interception systems. The data will be split into two sets: (1) Development activities: collected and properly pre-processed data resources (T4.3) and (2) Demonstration activities: all activities related to technology demonstrations will require data which can also be shared across	Transparency and accountability issues related to what data is chosen for training/testing and why. Dignity issues as data related to real people is involved.	Partners will be open about their rationale for why particular data sets are chosen for training/testing. Partners will give due regard to respecting the data coming from real people.	Medium

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

			project partners and end-user community (T9.1).			
	T4.7	Data and Remote Access Platform	In addition to T4.6, this task will be responsible for preparing data for field-testing (T8.3 and T8.4) in different phases of the project, as outlined in WP8 through 3 operational use-cases with increased complexity, also executed at field-tests: speech/video analysis use-case (M9), limited investigation use-case (M20), full investigation use-case (M30) (more details are given in Section 1.3.1, page 10, Grant Agreement). The task will ensure that the data is conforming to the specifications (T4.4) and that, if relevant, the data from social media is available (T4.3). In addition, continuous tests will be running at the LEA partners (T8.5), so that this task will run continuously.	Transparency and accountability issues related to what data is chosen for training/testing and why. Dignity issues as data related to real people is involved.	Partners will be open about their rationale for why particular data sets are chosen for training/testing. Partners will give due regard to respecting the data coming from real people.	Medium
WP5	Speech, text and video data analysis					

	T5.1	Initial Speech/NLP/Video Technologies	To enable a quick start of the project’s integration activities, PHO and SAIL will deliver production grade speech technologies to partners. Similarly, USAAR will provide its existing NLP technologies addressing some initial issue relevant for the target domain, and AIRBUS will provide baseline video technologies. All these will be made available with easy-to-use interfaces (i.e. as Linux scripts for laboratory use or REST-API services. or command line interface for the production use in WP7). The initial ASR modules will be provided in 8 languages (section 1.3.3.4 at page 17, Grant Agreement) corresponding to the scenarios defined in T2.1; more languages will be dynamically added.	Technical robustness issues related to whether Partner's machines can run the pre-existing software. Human agency and dignity issues regarding software decisions being premade. Diversity issues in terms of accessibility of the software.	Partners will ensure that they aid ensure that their software and datasets can work on others hardware. Diversity issues are somewhat alleviated as the software will be available in several languages and will have '*easy-to-use*' interfaces. Agency and Diversity issues are also somewhat solved as the use of pre-existing technologies was agreed during the ROXANNE proposal stage.	Low

	T5.2	Speaker Identification, Diarization and Role Recognition	The goal is to improve the performance of SID when used together with network analysis. Experiments will be conducted with neural end-to-end SID systems and suitable candidates will be selected for ROXANNE integration and productization (T5.7). SID will be enhanced by the use of conversational nature of speech data in network analysis, and on language identification to provide priors, select appropriate speaker models or perform adaptation or re-calibration of the SID system. This task also includes speaker diarization, and development of automatic approaches for detection of informal social roles. Speech technologies will make use of additional information coming from video analysis (T5.6) both for preparation of the training data, and during run-time.	Technical safety issues regarding neural networks being difficult (or potentially impossible) to understand. Diversity and non-discrimination issues in terms of whom speaker profiles will come from, and in what languages.	Safety issues can be somewhat mitigated by thoroughly testing the system to ensure as far as possible that it works as intended. Partners will ensure that the speaker profiles are as diverse as possible, and in multiple languages, in order to minimise discrimination issues, present in the system.	Medium

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

	T5.3	ASR for Network Analysis	ROXANNE will concentrate on the use of ASR in interaction with the network analysis. The participating partners will analyse the network data and contents of the conversation to develop a model of vocabulary propagation within a network. Having information about the context and the network structure of involved parties, this task will adjust the vocabulary probabilities and increase the quality of speech recognition (this can be carried out on a group, individual or combined level).	Privacy, data governance, and transparency issues due to partners having access to conversations. Technical safety issues regarding the linkages of speech recognition to network analysis.	Partners will follow good data governance practices to alleviate privacy, data governance, and transparency issues, and will thoroughly test the systems that are developed to ensure they work reliably and accurately.	Low

	T5.4	Entity Extraction and Geo-Information	Along with evidence provided by SID, ROXANNE will also rely on semantic analysis based on automatically generated transcripts. The core element and first step of any information extraction is the extraction of named entities, where the estimated reliability of the automatic annotation will be incorporated into the likelihood for the DNN training. To boost the performance, auxiliary information, e.g. from part-of-speech (POS) tags, will be used during training in a multi-task approach. In a second phase, this module will be expanded to handle speech recognition output, taking recognition errors into account. T5.4 will also manage the extraction of key information from gathered data (geo-locations, IP addresses, credit card numbers, etc.). For georeferenced data, geocoding and reverse geocoding will be performed as well as distance and path calculation.	Privacy and data governance issues generated by the extraction of gathered data. Transparency issues regarding how the neural network will work, and how '*auxilliary information*' will be included.	Partners will follow good data governance practices to alleviate privacy and data governance issues. The system will be well tested to ensure it works as intended.	Low

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

	T5.5	Relation Extraction and Discovery	From a given named entity (e.g. a person name) and a fixed list of predefined relations (e.g. born-in, married-to, employee-of, etc.) the corresponding second entity will be extracted. To address unavailability of annotated training data, we will again rely on a distant supervision approach. We will use related, auxiliary information, and confidences from the speech-to-text input. This task will also include the extraction of new relation types.	Privacy, data governance, and dignity issues arising from the identification of secondary persons. Transparency and accountability issues regarding how and how people are recognised by the system.	Partners will follow good data governance practices to alleviate privacy and data governance issues, in combination with being open about the reasons why a secondary person may be selected by the ROXANNE system and how this selection works to deal with transparency issues. Further, partners will be clear about who made the relevant decisions and why.	Low
	T5.6	Video Data Processing	The objective of this task is to develop or adapt specific computer vision based algorithms to process and analyse video to support the identification and recognition of the speakers: (i) content based indexing techniques to relate videos shot at the same location, (ii) semantic information extraction from video recordings to extract contextual information, and (iii) face verification. Face verification and video location verification will be tackled in priority. The objective of location verification is to build and demonstrate a video indexing pipeline allowing to link videos shot at the same location, leveraging contextual information extracted from object detection or	Privacy and data governance issues regarding individuals who are on video. Dignity issues in terms of people being recognised and data about them being processed through face verification. Transparency and accountability issues about why certain locations are chosen for video analysis linking and why.	Partners will follow good data governance practices to alleviate privacy and data governance issues. Partners will be open as to why particular locations are linked through video and the criteria for being linked and acknowledge their role in doing so. Dignity issues remain as an inherent drawback of using the system to recognise real people.	High

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

			semantic segmentation approaches.			
	T5.7	Production Speech/NLP/Video Technologies for NA	Industrial partners responsible for production-grade speech (PHO, SAIL), NLP (SAIL, ITML) and video (AIRBUS, ADITESS) technologies will continuously monitor the progress done by the research partners, correlate it with the user requirements (WP2) and results of early field tests (WP8), and include the promising results into their development cycles.	Data governance and transparency issues regarding how and why particular technological developments from ROXANNE will be used in the development cycles of technical partners. Accountability issues regarding who authorises ROXANNE technologies to be incorporated by the technical partners.	Partners will be open as to which ROXANNE technologies they are going to include in their development cycles, whilst following good data governance practices. The Coordinator will authorise technical partners to incorporate ROXANNE technologies.	Low
WP6	Network and relation analysis					
	T6.1	Fusion of Information for NA	This task aims to aggregate the data extracted from the WP5 analysis components to enable the extraction of relations between entities and for higher-level investigation. The following process will be developed: (1) Aligning data streams for time and granularity, using the ITML data fusion bus services. Specifically, for this task ROXANNE we will use a deep learning approach for data analysis and dynamic semantic level optimization to achieve accurate data fusion. (2) The data points will be analyzed for correlation as single networks, for example entities (people and	Technical robustness issues regarding the efficacy of data fusion. Transparency issues arising for the difficulties of understanding deep learning systems (neural networks). Privacy issues related to identifying people through video and geolocation. Diversity issues regarding whether access needs are taking into account for the user interface.	Partners will ensure that the system works accurately and reliably, and will test the system thoroughly so that it performs as intended. The ROXANNE system will be built in such a way that only persons of interest are focussed upon. Partners will also give due regard to the needs of potential end users.	Medium

			locations) co-occuring in images and persons co-occuring in data that have similar geolocation information, speaker ids identified and landmarks mentioned in speech data. The probabilistic formalism defined in this task will be bi-directional, i.e. allowing to produce confidences from speech/NLP/video analysis for the following NA, and on the other hand ingesting the probabilistic output from NA to influence speech/NLP/video mining. (3) A user interface will be created to allow for level-of-depth adjustment of the above as well as the selection of streams by LEA operatives.			
	T6.2	Construction of Crime Related Networks	This task will serve as a bridge between WP5 and W6. We will investigate and adapt state-of-the-art methods for semi-automatic and human/expert-supervised entity matching and linking across constructed networks to develop novel methods in criminal domains. Knowledge in criminal and terrorist studies will be exploited: the uncertainty in observed data, and heterogeneity of the data sources. The output will be a set of networks for each use case, allowing for more advanced analyses in the following tasks.	Dignity issues in terms of humans being subject to automated decision-making. Privacy issues due to the networks from the use-cases being developed with data from real people.	Partners will ensure that any automated decision-making is not overly-simplified. Partners will also supervise automated decision-making as far as is practicable. Partners will have anonymised (or pseudonymised) personal data as far as possible to minimise the privacy issues.	Medium

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

	T6.3	Multilayer and Cross-Network Structural Analysis	This task consists of analyses on networks constructed in the previous task. We will apply network approaches at three levels: (1) population level (e.g. connectivity, clustering and density analyses), (2) group level (e.g. subgroups and community detection algorithms), and (3) individual level (e.g. centrality, power and structural equivalence). We apply these approaches to the following analyses: (1) Multilayer/multiplex network analysis: the different networks provide a unique possibility to assess the multilayer nature of criminal activity. (2) Cross network analysis: the networks will be separately assessed in their topological structure to assess similarities and/or differences according to the data sources. We incorporate spatial and temporal context information to diversify available information leading to more insightful analyses.	Technical robustness issues relating to the efficacy of the system to deal with simultaneously analysing multiple complex organisations. Privacy and data governance risks arising from the large number of data subjects. Individual and Societal wellbeing issues due to significant risks of mass surveillance.	Partners will thoroughly test the ROXANNE system to ensure it works well. Partners will follow good data governance practices and will respect the privacy of data subjects as far as is possible in a project aimed at discovering suspected criminality. The risks of mass surveillance are limited by the amount of data available to project partners, but eventual customers may be less limited in their access to data.	Medium in project, high in eventual use.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

	T6.4	Multilayer and Cross-Network Behavioural Analysis	In this task we will develop and evaluate methods for identification, mining and analysis of activity pattern across networks. The work includes individual level analyses on the heterogeneous networks obtained from the T6.1 and T6.2. We will work on early detection of anomalies such as abnormal behavior, and on mining interaction patterns of the individuals within the network. These will be extended with information associated with the interaction pattern and context (e.g., time, location, and communicating channels, media, etc.) to obtain more insightful, actionable patterns.	Technical robustness issues regarding the efficacy of the identification and activity analysis. Privacy, dignity, individual and societal wellbeing issues arising from the treatment of persons as data points, and from treating '*abnormal behaviour*' as indicative of being of interest to criminal investigations.	Technical robustness issues can be mitigated through adequately testing the ROXANNE system prior to use. Privacy, individual and social wellbeing issues can be somewhat mitigated by thoroughly investigating the behaviours deemed '*abnormal*' to ensure that they definitively relate to criminality, and those behaviours which could be perfectly innocent are given less weight in identifying criminals. Dignity issues can be minimised as far as possible in the project by using anonymisation and pseudonymisation techniques where practicable.	High
	T6.5	Latent Subnetwork Detection	T6.5 will develop methods for detecting hidden (unobserved) subnetworks, missing node and link inference and completion of partially known interaction patterns. Some connections within a network are latent, carried out over inaccessible channels, or through unexpected patterns (criminals often use their relatives for communication). Some connections are only indirectly noticeable. These inferred sub-	Dignity issues due to people being treated as data. Privacy issues due to the invasiveness of investigating '*inaccessible channels*' and '*unexpected patterns*', also individual and societal wellbeing issues arising from the potential for innocent behaviours to be seen as indicative of criminality.	Partners will respect the privacy of data subjects as far as is practicable in a project aimed at finding and mapping criminality. Partners will ensure that the behaviours which are used to indicate criminality are definitively related to it and are not behaviours which could have an innocent explanation.	Medium

			networks are useful for enhancing the network construction steps, and also for improving network based techniques developed in other WPs.			
	T6.6	Subnetwork Shrinking	Not all nodes in a network are suspicious, and there exist only fuzzy boundaries. Reducing the network to the most relevant actors decreases distraction to the investigators and can uncover obscured patterns. In this task we will develop probabilistic risk estimation models for adjustable shrinking of the network to the most relevant nodes at a particular threshold. This task is essential for the network relation visualization that will enable LEA operatives focus on the critical findings and relations.	Transparency and data governance issues regarding how the networks will be narrowed down, and what happens to the data that is left out.	Partners will be open about the process for narrowing down networks to focus on persons of interest. Partners will follow good data governance practices related to unused data.	Low

	T6.7	Systematic Assessment of SLT and Relation Analysis to Criminal NA	This task will systematically compare the contribution of the data, analyses, information, and techniques provided by ROXANNE in supporting processing of investigation. The assessment will start with analysis of the "classic" criminal networks (T6.1) and based on relational information commonly used in classic criminal network analyses (e.g. telephone contacts, wiretaps or meetings). For each use case, three levels will be assessed: whole network, subgroups and individual nodes. Then, analysis of the "advanced" criminal networks (T6.2 to T6.6) will be performed using similar metrics.	Transparency and data governance issues related to how the three levels of criminality are chosen, and the distinction between classic and advanced criminal networks. Privacy issues related to access to information on individual nodes (people)	Partners will be open about how the networks are narrowed down to each level. Partners will also respect the privacy of each person involved as far as is possible when building new technologies for investigating suspected criminals.	High
WP7	Integration and Visualisation of results					
	T7.1	Design and Definition of the ROXANNE System Architecture	The objective of this task is to define an open architecture based on open standards in order to ensure the system. TRI will ensure that the architecture definition follows PbD and complies with WP3. The success of field tests and user-training highly depends on the precise definition of use-cases, therefore this task is tightly interrelated with T2.4.	Dignity and diversity issues if a wide range of views are not considered. Transparency issues if system is highly-complex. Accountability issues if participant actions are not logged. Robustness and data governance issues if people working on project are not adequately trained. Environmental issues if the architecture if unnecessarily complex and	Partners will treat each other with respect, ensure adequate training is provided, develop the system to be as simple as possible, log all of their activities related to the project, and consider the energy consumption of the resulting system.	Low

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

				uses more energy than necessary.		
	T7.2	User Management and Access Control	T7.2 will build on T4.5 and develop all the platform components necessary in order to secure data exchange and enable simultaneous operations by multiple users with different rights. T7.2 will implement a central authorization and authentication service and logging mechanisms. Additionally, T7.2 will establish all the procedures and technological enablers in order to ensure security and trust across the entire infrastructure.	Potential dignity, discrimination, and wellbeing issues if no common policy for user access is agreed. Potential security, data governance, and accountability issues if people are not adequately trained in good practice. Also, potential discrimination issues if partners do not agree methods of interoperable working between organisations.	Partners will develop policies on access to the development platform and good practice whilst using it. Partners will also ensure interoperability between organisations.	Low
	T7.3	Run-Time Data Visualisation and Exploratory Analysis	This task aims to develop advanced visualisation techniques for visual data exploration using scalable data visualisation approaches and tools that will enable easy transition from one scale to another or from one form of aggregation to another. Moreover, enhanced configuration and collaboration features will enable the users (both research/industry as well as LEA personnel) to share visualisations, using configurable chart representations of datasets and advanced filtering capabilities through a single visualisation and monitoring toolkit.	Liberty, data governance, diversity, and individual wellbeing issues if the access needs and preferences of testers/end-users are not taken into account in terms of how they need/want data to be visualised. Safety issues if system not adequately secure. Transparency issues if system weaknesses are not noted. Accountability issues if there is a lack of human oversight.	Partners will listen to potential testers/users of the system rewarding their needs/preferences. They will build the system in a secure way, note any weaknesses, and enable human oversight.	Low

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

	T7.4	Secure Data Export and Exchange	This task entails the design and implementation of a generic mechanism to export data for the use in external applications. T7.4 will implement the services needed for the secured exchange of information with peer LEAs and its potential international organisations - a data selection mechanism, with which LEAs will be able to (i) request information from peer entities and (ii) select internal information to be exported to third parties. T7.4 will implement the means of generating templates for data transformation, minimizing the cost in resources for transformation between different data sharing standards (i.e UML) or established databases with verified content (i.e. ICSE database maintained by INTERPOL, presented at page 8, Grant Agreement).	Dignity issues if preferences on data storage/transfer are ignored. Data Governance, Transparency, and Discrimination issues all present with regard to how choices to provide data are made, and the complexity of the system. Who makes these decisions also generates accountability issues. Cybersecurity issues are also present with regard to how secure the data transfer system is.	Partners will develop a policy on what data can be provided and on what grounds, with a named individual who made the decision, to alleviate most issues. Partners will also validate and verify the secure nature of the data transfer capability, and ensure it is simple enough to use.	Low

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

	T7.5	Integration, ROXANNE System/Platform Setup and Maintenance	In order to provide a platform on which technical advances can be evaluated by end-users (and project partners in general) a specific instance of WebLab will serve as the ROXANNE Platform in three different stages of maturity. The outcomes of WP5, WP6 and WP7 will be integrated into WebLab and be provided as an initial testbed in M9 (light integration allowing to show the different capabilities that can be provided by technical partners), as an enhanced prototype at M20 (for the 2nd field test) and as the final platform at M30 (also used for final evaluations).	Liberty, discrimination, and wellbeing issues if not all partners can/want to use WebLab. Security and reliability issues if WebLab is inadequate. Data governance and Transparency issues if participants edited/delete other people's work. Accountability issues if nobody is specifically responsible for the collective work.	The use of WebLab has already been agreed by partners and so it should be desirable/possible for all partners to use in addition to being secure and reliable. Transparency and data governance issues will be solved if colleagues adopt good data governance practices and log their activities. Accountability issues resolved if someone is responsible for the use of WebLab (WP Lead?).	Low
	T7.6	Integration of Feedback from End-Users	This task deals with modifications made to the integration and visualization system based on feedback from participants of the meetings with LEAs, in particular the field-test meetings. In this respect it constitutes the link between the work packages WP7 and WP8. Feedback of end-users can be integrated for each of the 3 versions of the ROXANNE Platform as delineated in T7.5.	Dignity, robustness, transparency, discrimination, and wellbeing issues may be present if submissions are not treated fairly and openly. Privacy issues if personal data is included in submissions. Accountability issues if nobody is charged with overseeing submissions.	Partners will approach submissions with an open mind and with regard to fairness. Minutes of meetings are taken to ensure transparency and accountability for decisions. Partners are obliged to delete any personal data which the are provided with but do not need as part of privacy by design and Art.5(1)(c), GDPR.	Low
WP8	Field Tests, user training and continuous testing					

	T8.1	Development of End-User Validation and Performance Test Methodology	An end-user validation and performance test methodology (quantitative and/or qualitative) will be developed, which will allow evaluating the developed speech/text/video analytics and network analysis tools and technology both separately and combined. The developed methodology will ensure that we have evaluated the right system features with the appropriate components, based on a sound scientific methodology which will produce actionable results for the further enhancement of the ROXANNE platform.	Robustness and transparency issues in terms of how the methodology is developed and how it will affect other work.	Partners will thoroughly test the methodology to ensure it works as intended.	Low
	T8.2	End-User Training	This task will develop a set of training materials (manuals, physical and/or online training, etc.) that will assist the end-users to use the ROXANNE platform. The trainings will be activated before each field test (T8.4) with an e-learning platform (+webinars) aligned with three 3 phases of field-tests (as indicated on Figure 3.2): M6, M17, M27 (i.e. 3 months before field-tests). For targeted and effective theoretical and practical training, the e-learning platform will combine a set of interactive means (i.e. documentation, presentations, videos, simulation). The web-based e-learning platform	Technical robustness issues regarding the efficacy of the e-learning platform. Human agency, liberty, dignity, and individual wellbeing issues related to the power relationship of trainer/trainee. Privacy and data governance issues relating to the training platform collecting personal data.	Partners will thoroughly test the e-learning platform to ensure it works as intended. Partners will also be cognisant for any potential power relationship and develop the platform so that trainees retain their freedom due training activities. The platform will also be constructed according to privacy by design principles.	Low

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

			will be hosted on the KEMEA server and case-work produced in WP2 will be used to shape sample training scenarios.			
	T8.3	Field Test Planning	This task will ensure that the developed solutions are tested under realistic conditions and use cases. Planned field test will consider: (1) hosting of the IT equipment in LEA premises and ensuring access to the real data (see T4.1). (2) Provision of LEA staff to facilitate field tests, (3) Event dissemination plan, other materials and event documentary movie for large audience, (4) Field-test day's logistics and (5) Definition of the test strategy and test plans.	Human agency and dignity issues related to partners deciding upon what colleagues should do at field tests.	Partners will respect the agency and dignity of colleagues.	Low

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

	T8.4	Design, Implementation of Field-Tests	Three field-tests combined with continuous testing (described in T8.5) will evaluate the developed technology. More details on planned 3 operational use-cases, aligned with 3 field-tests (and also continuous testing) were given in Section 1.3.1 (page 10, Grant Agreement): - Field test 1: speech/video analytics with preliminary NA (M9, at KEMEA premises) - Field test 2: Reduced complexity investigation use-case, first full demonstration of ROXANNE (M20, at NFI premises) - Field test 3: Full complexity investigation use-case, second full demonstration of ROXANNE (M30 at INTERPOL premises). Specific evaluation sessions will also take place after the end of each field-test, ensuring that the evaluation plans are adequately carried-out and specific recordings are being kept for later analysis of results. As anticipated in T8.2, field-test events will host training activities as well.	Technical robustness and safety issues regarding the efficacy of the system. Human agency, dignity, privacy, data governance, transparency, and individual wellbeing issues related to the actual use of the system. Also, potential diversity and discrimination issues if system does not accurately represent the populations it is being tested with.	Partners will thoroughly test the system to ensure it works as intended. Partners will also take note of the issues highlighted in other tasks to ensure that other issues are minimised.	Low if previously outlined issues are dealt with

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

	T8.5	Continuous Testing	Besides the three field-test events organized by three different LEAs, ROXANNE will apply a process of executing human-operated tests as a part of evaluating the developed technology in the project. All project end-user partners have a dedicated budget to test the platform on real operational data. The main objective is to continuously deploy and evaluate the technology on realistic criminal cases and obtain immediate feedback for technical partners to allow further improvements of the ROXANNE system.	Privacy, data governance, transparency issues related to use of real criminal case data. Human dignity and individual wellbeing issues relate to reducing real people to data points. Discrimination issues if platform does not use diverse data sets.	LEA Partners will ensure that any infringement of the privacy of real individuals complies will applicable legal and ethical considerations when conducting criminal investigations. Technical partners will ensure that the platform reflects diverse populations.	Low if previously outlined issues are dealt with
	T8.6	Field Test Results Analysis and Evaluation	Goal of this task is to analyze overall results and feedback obtained from field-tests and continuous testing, thus measure system performance. Objective and subjective feedback collected from internal (consortium) and external LEAs attending the field test events will be analyzed. All the developed solutions will be presented to a large number of external LEAs, so that the technology is feasible in a variety of LEA's investigation environments.	Fairness issues in terms of how the results from LEAs/non-LEAs are treated. Data governance and transparency issues regarding how data is chosen for display. Dignity, individual wellbeing issues if data on real people is openly displayed.	Partners will treat results from all tests in a fair and open manner. Partners will also respect the privacy of people subject to the criminal investigations.	Low
WP9	Dissemination, exploitation and communications					

	T9.1	Conduct Stakeholder Analysis and Compile a Stakeholder Contact List	The success of our project depends on our reaching out to stakeholders who will have an interest in and be able to use the results of the project. The consortium will develop a taxonomy of the different ways of grouping stakeholders (demographically, geographically, socio-economically, etc.), their needs, interests and/or requirements, and the size of the stakeholder group. The partners will compile a stakeholder contact list from contact data openly available on the website of the stakeholder's organisation. We will inform the stakeholders of the project's research and results. The stakeholder list will be finalized at 1st field-test (M9), but later updated.	Privacy, data governance issues regarding collection of personal data. Diversity issues related to the make-up of the stakeholder contact list.	Partners will follow the GDPR and national data protection legislation to ensure privacy of stakeholders is respected. Partners will ensure that the stakeholder list is as diverse as possible.	Low

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

	T9.2	Elaborate the Dissemination and Exploitation Plan, IPR Management	Partners will elaborate the plan for dissemination and exploitation of results, the initial draft of which is in section 2.2(a) of Grant Agreement. The plan will describe the project's key exploitable assets and, drawing on the initial results of T9.1, who is most likely to use our results. We will define the exploitation objectives based upon a review of the current market-place for SLT, NLP, VA and NA tools and services especially oriented for investigations. The plan will define key messages, select appropriate channels (including relevant conferences, fairs and events) to convey those messages to the target stakeholder groups and explain the means and ways by which we will interact with and respond to stakeholders. T9.2 will coordinate the management of IPR and patent search as well, and to set and execute the exploitation strategy of the consortium.	Data governance issues regarding what data/information can be disseminated. Diversity and non-discrimination issues related to whom the information is disseminated to and who are targeted as prospective customers.	Partners will ensure they only disseminate information which they are allowed to and do so in a fair and diverse manner.	Low

	T9.3	Elaborate the Plan of Communication Activities	Partners will elaborate the plan for communications activities (section 2.2(b)) by month M4, with a revision if necessary at month M18. The plan will describe the activities we intend to carry out to inform the public, the news media and other stakeholders about the project and its activities over the three-year life of the project. The plan will describe the tools we will use to communicate our messages to each of the key stakeholder groups.	Transparency issues regarding how much information on the ROXANNE tools will be shared.	Partners will respect ROXANNE colleagues by only revealing information that will not harm commercially sensitive work. Partners will respect stakeholders by providing them with enough information so that they can have an accurate picture of how the tools work and whether they could be used by their organisation.	Low
	T9.4	Promote the Project Identity and the Project's Website	TRI will create a corporate identity for the project to ensure a common graphic line (project leaflet, website, presentation templates etc.) for all communication materials produced by the consortium. IDIAP will create the project's website (dedicated budget), to communicate, inform, create dialogue and promote use of the project results among the target stakeholder groups (researchers, industry, academic, media, policy makers, civil society organisations, LEAs, etc.). The website will be continuously updated, offering bi-monthly newsletters and the documents to be shared among partners and public as well as an interactive blog. T9.4 will also establish social media channels	Human agency, dignity, and individual wellbeing issues regarding ROXANNE workers being linked to a corporate identity they have little or no control over.	Partners will be open about their plans for the ROXANNE corporate identity, and will give due regard to the opinions of colleagues within the consortium.	Low

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

			and will push project's announcements through them. At M9, project's brochure will be released to be available at first field-test event, summarizing the technical approach and activities of ROXANNE.			
	T9.5	Prepare and Use Dissemination and Communication Materials	The partners will prepare various dissemination and communications materials, as detailed in the plans in D7.2 and D7.3, which will be circulated via the traditional press, social media, specialised blogs and magazines, and the project's website. Additional project information and frequent updates on the most recent news and project activities will be posted regularly on the project's accounts on social media sites (Facebook, Twitter, LinkedIn, etc.). A report (D9.4) will collect the various dissemination, exploitation and communications products and services created by the consortium (e.g., presentations, webinars, social media accounts, videos, etc.) and report on their impact and dissemination. It will also report on the website activity and the number of contacts. TRI will produce three short videos (60-90 seconds) to promote the project.	Transparency and accountability issues regarding how the data generated by social media dissemination will be used later.	Partners will be cognizant of how social media platforms can use the data they disseminate, and will not use these platforms more than necessary.	Low

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

	T9.6	Exploit the Project's Results	The project will facilitate stakeholder use of the project's results in several ways, including the following: It will (1) inform stakeholders about the project's results, (2) conduct webinars (workshops) to help stakeholders understand how they can use the results, (3) offer "how-to" guides on the project website, (4) offer an online helpline where stakeholders can text their questions, (5) participate in professional and/or standards bodies, (6) trademark its services, (7) copyright certain deliverables, (8) press releases, (9) trades/events, etc.	Privacy and data governance issues related to how partners will deal with data they acquire through dissemination. Agency issues relating to risk of 'how-to' guides affecting freedom of thought. Transparency and accountability issues regarding what ROXANNE tools will be trademarked/copyrighted, and how this will be enforced, and how this could affect partners/users.	Partners will follow the GDPR and national data protection legislation. Partners will be open that the suggested uses of ROXANNE are not their only uses. Partners will be open about the effects of trademarking/copyrighting ROXANNE tools, and enforcement mechanisms.	Low
	T9.7	Convene the Project's Final Conference	The consortium will convene a final conference for journalists, industry, civil society organisations, legal experts, associations, advisory board members and other stakeholders. The partners will use the conference to showcase the project's website, its results and its recommendations. The partners will prepare a summary of the project results as a handout (a 16-page booklet) to stakeholders at the conference (and others after the conference).	Privacy and data governance issues regarding holding personal data on conference attendees.	Partners will follow the GDPR and national data protection legislation.	Low

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

	T9.8	Prepare Articles for Peer-Reviewed Journals and Conference Presentations	The academic partners will extensively publish in journals and at top conferences. Input from industrial partners and end-users will motivate the publications. We will count on industrial co-authors and all partners participating in this Task.	Dignity issues regarding the work of consortium partners being recognised in publications/conference presentations.	Partners will give due regard to the work of their colleagues, and how this impacted on any work they publish.	Low
	T9.9	Policy Recommendations	Drawing on the results of all previous work packages, the partners will formulate the project's recommendations to key stakeholders, including LEAs, policymakers, academics, researchers and media, among others. The partners will address specific recommendations to specific stakeholders for the steps they can take to ensure ROXANNE platform will address technological, legal, data protection, ethical and societal issues that have become apparent during the project.	Transparency issues related to how the recommendations are drawn up.	Partners will take minutes of all meetings which will be available for all partners to view.	Low
WP1 0	Ethics Requirements					

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

	D10.1	Procedures for Identifying/Recruiting Research Participants	The procedures and criteria that will be used to identify/recruit research participants must be submitted as a deliverable. The informed consent procedures that will be implemented for the participation of humans must be submitted as a deliverable. Templates of the informed consent forms and information sheets (in language and terms intelligible to the participants) must be submitted as a deliverable.	N/A	N/A	N/A
	D10.2	Opinions of Ethics Committees on Research with Human Participants	Copies of opinions/approvals by ethics committees and/or competent authorities for the research with humans must be submitted as a deliverable.	N/A	N/A	N/A
	D10.3	Check if Special Derogations on Rights of Data Subjects Established under National Law	The beneficiary must check if special derogations pertaining to the rights of data subjects or the processing of genetic, biometric and/or health data have been established under the national legislation of the country where the research takes place and submit a declaration of compliance with respective national legal framework(s). This must be submitted as a deliverable.	N/A	N/A	N/A

	D10.4	Confirmation of Lead Institution DPO policy	The host institution must confirm that it has appointed a Data Protection Officer (DPO) and the contact details of the DPO are made available to all data subjects involved in the research. For host institutions not required to appoint a DPO under the GDPR and the Directive 2016/680, a detailed data protection policy for the project must be submitted as a deliverable.	N/A	N/A	N/A
	D10.5	Description of Measures to Safeguard Rights and Freedoms of Data Subjects	A description of the technical and organisational measures, including anonymisation/pseudonymisation techniques, that will be implemented to safeguard the rights and freedoms of the data subjects/research participants must be submitted as a deliverable. A description of the security measures that will be implemented to prevent unauthorised access to personal data or the equipment used for processing must be submitted as a deliverable.	N/A	N/A	N/A

	D10.6	Confirmation of GDPR Compliance in Case of Data Transfer Outside of EU	In case personal data are transferred from the EU to a non-EU country or international organisation, confirmation that such transfers are in accordance with Chapter V of the General Data Protection Regulation 2016/679, must be submitted as a deliverable. In case personal data are transferred from a non-EU country to the EU (or another third state), confirmation that such transfers comply with the laws of the country in which the data was collected must be submitted as a deliverable.	N/A	N/A	N/A
	D10.7	Informed Consent Procedures	Detailed information on the informed consent procedures in regard to data processing must be submitted as a deliverable. Templates of the informed consent forms and information sheets in regard to data processing (in language and terms intelligible to the participants) must be submitted as a deliverable.	N/A	N/A	N/A
	D10.8	Confirmation of Lawful Basis for Further Data Processing	In case of further processing of previously collected personal data, an explicit confirmation that the beneficiary has lawful basis for the data processing and that the appropriate technical and organisational measures are in place to safeguard the rights of the data subjects must be submitted as	N/A	N/A	N/A

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

			a deliverable.			
	D10.9	Explanation of How Profiled Individuals will be Notified	In case the research involves profiling, the beneficiary must provide explanation how the data subjects will be informed of the existence of the profiling, its possible consequences and how their fundamental rights will be safeguarded. In case of proactive profiling leading to police activities the applicant shall refer to existing legal frameworks and safeguards to ensure that individual fundamental rights are respected. This must be submitted as a deliverable.	N/A	N/A	N/A
	D10.10	Legal Basis for Processing Criminal Conviction Data	In case personal data relating to criminal convictions and offences are processed, an explicit reference to the Union or Member States law(s) authorising their processing with provision for appropriate safeguards for the rights and freedoms for data subjects and description of technical and organisational measures adopted to comply with these safeguards must be submitted as a deliverable.	N/A	N/A	N/A

	D10.11	Evaluation for Ethical Risks Related to Data Processing	The beneficiary must evaluate the ethics risks related to the data processing activities of the project. This includes also an opinion if data protection impact assessment should be conducted under art.35 General Data Protection Regulation 2016/679 and/or art.27 of the Directive 2016/680. The risk evaluation and the opinion must be submitted as a deliverable.	N/A	N/A	N/A
	D10.12	Appointment of an Ethics Board	Due to the severity of the ethics issues raised by the proposed research, the members of the Ethics Board (including relevant independent expertise to monitor the ethics issues in this project and how they are handled) must be appointed. The Board must be consulted at least on the following points: potentially processing of sensitive data (behavioural tracking), social media data processing and risk of misuse/mass surveillance. This must be submitted as a deliverable.	N/A	N/A	N/A
	D10.13	Report by Ethics Board	A report by the Ethics Board must be submitted as a deliverable at month 4.	N/A	N/A	N/A
	D10.14	Report by Ethic Board	A report by the Ethics Board must be submitted as a deliverable at month 12.	N/A	N/A	N/A
	D10.15	Report by Ethics Board	A report by the Ethics Board must be submitted as a deliverable at month 30.	N/A	N/A	N/A

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635. No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the ROXANNE project partners. © 2019 – All rights reserved.

	D10.16	Report on Preventing Misuse of Research Finding and Avoiding Mass Surveillance	A report including risk assessment and details on measures to prevent misuse of research findings and that also addresses how the software tools (in particular the social media analysis and deviant behaviour detection tools) avoid the risk of mass surveillance of the general public and/or specific groups of people. This must be submitted as a deliverable.	N/A	N/A	N/A
	D10.17	Detail of AI/Data Mining System, Human Roles, Avenging Algorithmic Biases and Justification of Results	The beneficiary shall provide details on the Artificial Intelligence/Data Mining system and related decision making procedures including information about human actors roles and responsibilities. The beneficiary must also describe a set of precautions to eliminate or mitigate potential algorithmic biases and explain how the model will be able to justify the results it has provided for specific situations. This must be submitted as a deliverable.	N/A	N/A	N/A