Minimisation of Incidental Findings, and Residual Risks for Security Compliance: the SPIRIT Project

Pompeu CASANOVAS [1,2,3], Nicholas MORRIS [1], Jorge GONZÁLEZ-CONEJERO [3] , Emma TEODORO [3], Rick ADDERLEY [4]

[1] *La Trobe Law School, La Trobe University, Melbourne, Australia*
[2] *Data to Decisions Cooperative Research Centre, La Trobe University*
[3] *Autonomous University of Barcelona (IDT), Spain*
[4] *A E Solutions (BI) Ltd. and Leicester University, UK*

Abstract. This paper introduces the policy for minimisation of incidental findings and residual risks of the SPIRIT Project. SPIRIT is a EU H2020 Security project, aimed at browsing relevant sources, including the so-called "dark web". It proposes a semantically rich sense-making set of tools aimed at detecting identity fraud patterns. It provides "Technologies for prevention, investigation, and mitigation in the context of fight against crime and terrorism" for the use of LEAs in Europe. According to GDPR, some protections must be put in place. We explain how we planned and designed them. Specifically, we turned incidental findings into an incidental risks policy, planned a risk mitigation strategy (ongoing privacy preserving algorithm development), and set a dynamic DPIA.

Keywords. Security, EU Project SPIRIT, privacy, residual risks, incidental findings

1. Introduction

The Internet has caused significant shifts in the patterns of criminal activity, enabling organised crime groups to access a large pool of victims, obscure their activities, and carry out a diverse range of criminal acts on a much larger scale than ever before. Frequently, these criminal activities are committed remotely and with anonymity, making detection and prosecution more complex than crimes that do not rely on the Internet and the virtualised modus operandi. Thus, for Law Enforcement and control agencies (collectively LEA's), the detection of identity fraud and other criminal activities involving the internet is an increasingly complex task.

The SPIRIT project[1] addresses the issues above by proposing a semantically rich sense-making set of tools aimed at detecting identity fraud patterns. It provides "Technologies for prevention, investigation, and mitigation in the context of fight against crime and terrorism" for the use of LEAs in Europe. These technologies enable complex associative searches over all sources relevant to the current investigation, correlate information from multimedia data, understand information which involves uncertainty, and structure and manipulate information into a unified view of the available evidence over a persisted, searchable knowledge base. They involve the use of large quantities of personal data accessed from social media and other sites by the use of web crawlers and similar technologies.

The European Union has numerous regulations which protect citizens from the inappropriate use of their personal data, which we summarise below. In order to minimize the risk that data might be inadvertently used or accessed by LEAs in a way which contravenes these regulations, we have therefore developed risk minimization procedures. These involve the careful definition and grouping of incidental risks, the development of mitigation policies, and the identification of residual risks.

2. Appropriate Safeguards

The processing of personal data for scientific purposes is addressed specifically in Article 89 (1) of the European Union General Data Protection Regulation (GDPR) [6]. This article, in line with Recital 156, states that:

> Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject.

GDPR also sets out the principle of data minimization in Article 85 (1c), as follows: 'Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')'.'Appropriate safeguards' have been defined by the Article 29 Working Party [1] (replaced by the European Data Protection Advisory Board[2]) as data minimization, anonymisation and data security, with anonymisation the preferred solution if the research purpose cannot be achieved without processing personal data. Transparency[3] is suggested an additional safeguard when it is not possible to obtain specific consent for the research.

Minimising Risks in the use of personal data is also covered by the Regulation, which states at Recital 78 that this should involve:

[1] SPIRIT—Scalable privacy preserving intelligence analysis for resolving identities, a project funded under the European Commission Horizon 2020 programme.

[2] See: https://edpb.europa.eu/edpb_en

[3] See: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

> minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor data processing.

Legislation differs in Member States on what type of personal data police forces are allowed to access, under which circumstances and through what procedures, although EU Directive (EU) 2016/680 [7] may harmonise it.[4] Police forces must strictly adhere to these requirements, and they do, as the risk is to have the criminal proceedings invalidated later on in court, due to the breach and the subsequent harm on the fundamental rights and freedoms of citizens.

The Recommendation CM/Rec(2017)6 provides further guidance [8]. Articles 7-10 list the protections to be considered:

> 7. Special investigation techniques should only be used where there is sufficient reason to believe that a serious crime has been committed or prepared, or is being prepared, by one or more particular persons or an as-yet-unidentified individual or group of individuals.
>
> 8. Member States should ensure proportionality between the special investigation techniques used and the legitimate aims pursued. In this respect, when deciding on their use, an evaluation in the light of the seriousness of the offence and the intrusive nature of the specific special investigation technique used, should be made. Also the urgency and general complexity of the case could be considered.
>
> 9. Member States should ensure that competent authorities apply less intrusive investigation methods than special investigation techniques if such methods enable the offence to be prevented, detected, investigated, prosecuted and supressed with adequate effectiveness.
>
> 10. Member States should take appropriate legislative measures to permit the production of evidence gained from the lawful use of special investigation techniques before courts. Procedural rules governing the production and admissibility of such evidence shall safeguard the rights of the accused to a fair trial.

The SPIRIT project contains carefully-designed safeguards to ensure that it complies with these requirements.[5] Relevant ethical issues have been analysed from the SPIRIT perspective and include recruitment of participants, information to participants, informed consent, data handling during research activities and the creation of an Ethical Advisory Board (EAB).[6]

Monitoring activities within the SPIRIT Project are being carried out by internal and external authorities. Internal authorities are (i) the ethical and legal lead partner of the

[4] Art. 63.1 sets the timeline: "Member States shall adopt and publish, by 6 May 2018, the laws, regulations and administrative provisions necessary to comply with this Directive. They shall forthwith notify to the Commission the text of those provisions. They shall apply those provisions from 6 May 2018."

[5] See SPIRIT Deliverable 9.1, Informed Consent (WP9)

[6] For detail of the activities of the EAB, see SPIRIT Deliverable 9.3, Ethics Advisory Board (WP9. Members of the EAB are: Ugo Pagallo (Chair), Lilian Mitrou, Virginia Dignum, Giovanni Sartor, and David Watts.

project; and (ii) the Data Protection Officer, specially appointed to ensure strict compliance with the EU and national legal data protection frameworks. The external authorities are (i) the Ethical Advisory Board (EAB)AB, (ii) the Ethical Committees of the LEAs participating in the project, and (iii) National Data Protection Authorities.

Due to the nature of research activities, and in particular the processing of personal data that will be conducted during the SPIRIT project, the obligation to notify Data Protection Authorities has been defined in accordance with (i) the General Data Protection Regulation (GDPR), (ii) the Law Enforcement Directive (LED), and (iii) the applicable national legal frameworks in which processing of personal data will take place.[7]

3. Incidental Findings and Residual Risks

3.1. Appropriate safeguards

To ensure that the use of SPIRIT technologies complies with these regulations, and with the relevant laws of each member state, we have developed a set of measures for the reduction of incidental findings and residual risks: (i) a policy for re-identified data, (ii) a privacy preserving algorithm development process, (iii) a Privacy by Design (PbD) approach, (iv) an incidental risks mitigation policy.

In order to quantify the various risks involved, we have developed a spreadsheet-based model which seeks to calculate the overall risks which may be faced by the SPIRIT system, both before and after policies have been implemented to mitigate these risks. This characterises i*ncidental risks* as the risks of misuse of the system caused by internal and external factors. These risks can be mitigated (reduced) by the use of suitable *policies*. The risks that remain after these policies have been implemented and taken full effect we term *residual risks*.

In order to identify possible sources of incidental risks we have reviewed privacy and data protection inquiries, press coverage, and the academic literature on the subject. This investigation has focused particularly on the recent literature and experiences following the introduction of GDPR in 2016 (enacted on May 25th 2018), and the Directive (EU) 2016/680 on the prevention, investigation, detection or prosecution of criminal offences. The review also built on the findings of a previously-completed Data Protection Impact Assessment (DPIA).[8]

[7] Notification procedures are defined in SPIRIT Deliverable 9.4, Notifications to National Data Protection Authorities (WP9).

[8] SPIRIT *Reply to the Ethics Second Assessment Report*, April 30th 2018, section 9.3.3.

3.2. Incidental findings

The notion of incidental findings originated in medical and genetic research.[9] Hence, it is a bio-ethical notion applicable to physical diagnosis, radiology, and brain image exploration (MRI) [13].

In a broad sense incidental findings include both false positives and marginal findings with no clinical relevance occurring within doctor-patient relationships. In a narrower sense, (i) they occur in participants during a scientific study, (ii) they potentially might affect the health or reproductive capacity of participants, (iii) they were not intended in the study's aim [11]. We can differentiate [5] between (i) incidental findings, (ii) secondary findings (as a result of the first ones), and (iii) discovery findings. The handling of "incidentalomas" (abnormalities revealed during imaging, which were not accompanied by any symptoms) raise ethical concerns in all three cases.[10]

3.3. Application to security and policies

Application of this literature to the security field requires some adjustments, due to the informational processing character of the risks and the potential harm caused to the rights and everyday life of citizens. Identity management, privacy and data protection, and the possibility of social and political discrimination raise more issues that parallel but do not equate to the possible harms in biological, genetic, and medical sciences.[11] Some more constraints apply in the scenarios created in security and policing environments because of the imbalance of power between the different stakeholders. I.e. LEAs are usually compliant with internal and external best practices, regulations and legislation. They are supposed to follow appropriate procedures, and it is generally the case that they do so. But incidental policy guidelines should reflect all possible harms, including those caused by intentional behaviour (for instance, vendettas, bribery and conflicted personalities).

In keeping with these observations, we have adopted not only a top down, but also a *middle-out approach*, in which social engineering can be combined with systemic measures to monitor and control both the system, the human beings involved in its management, and the framework in which hazards occur and residual risks remain. [12] extends Levenson's STPA (Systems-Theoretic Process Analysis) to security, STPA-SEC. They reframe the security approach based on guarding against cyber-attacks into a socio-technical perspective focusing on vulnerabilities that allow disruptions to propagate throughout the system. This would reduce risks to residual risks.

[9] According to [4] incidental findings became an issue within genomic medicine in the transition from targeted genetic testing to genome-scale screening testing. Targeted genetic testing consisted of probes, which targeted particular sequences in the genome known to be linked to diseases for which the test was performed.

[10] Although the influential report *Anticipate and Communicate. Ethical Management of Incidental and Secondary Findings in the Clinical, Research, and Direct-to-Consumer Context* published by the Presidential Commission for the Study of Bioethical Issues (USA Presidential Commission) in December 2013 treats only incidental and secondary findings.

[11] SPIRIT. Reply to the Ethics Second Assessment Report, April 30th 2018, section 9.3.3.

Chance and damage are uncertain in IT security for four main reasons [10]: (i) vulnerabilities change frequently, (ii) the IT environment itself changes continuously, which changes both the probability and the potential damage, (iii) the chance that a threat causes damage is influenced by unknown external factors, and (iv) the cost of the damage is hard to estimate.

3.4. Risk Mitigation

The analysis of hazards should include as many cases as possible to be useful to internal and external controllers and to minimise the risks. This is another way of stating that (i) compliance with laws, regulations and court assessments, (ii) technological conformance with existing standards, and (iii) congruence with ethical principles, could be better achieved if based on empirical knowledge and reasonable estimation.

Following completion of the DPIA, a variety of mitigation procedures have already been planned in a privacy preserving algorithm development: (i) to ensure that the privacy of individuals is safeguarded- both during the validation and training phases and in the final technology resulting from SPIRIT- in the development phase, human intervention points will be built into algorithms, methods and crawlers so that, when used, it will provide transparent levels of authority to progress the investigation into open source data or closed data such as emails, closed social network profiles, bank records, etc., and (ii) police forces will have to enter into the investigation the relevant authorisations, either from a superior officer or from a judicial authority, according to the different legislations in the different countries.

We have concluded, for the LEAs involved in SPIRIT, that risks related to the lawfulness of the overall process; to purpose specification; and to access rights have been sufficiently mitigated. However, risks related to data minimisation; data accuracy; accountability; and data security require further attention, including the use of procedures embodied in the SPIRIT project.

The Police and Justice Authorities Directive (2016/680/EU) [3] provides useful guidance on the identification and quantification of incidental risks, as follows:

> The likelihood and severity of the risk should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, through which it is established whether data-processing operations involve a high risk. A high risk is a particular risk of prejudice to the rights and freedoms of data subjects.

4. Empirical estimation of residual risks

4.1. Incidental risk mitigation model

Consistent with these objectives, we have grouped the remaining incidental risks into five *sources* – those emanating from Individual, LEA, Political, and External actions, and those which comprise Reputational Attacks on the system.

For each of the *categories* of risk identified, for each of the sources of risk, we seek estimates of the likely incidence of a system failure (factor A) occurring. For the present, we have three levels of severity (factor B) - high (H), medium (M) and low (L). A weight is also applied to each category for each source, indicating the importance of that category in the overall probability of the relevant source causing a failure (factor C). ‘Failure’ in this sense includes lack of compliance with European regulations, and unauthorised breaches of privacy or human rights.

Cross-multiplying A*B*C gives us a combined probability of the risk category eventuating in a system failure. Adding the probabilities across all sources gives us an overall probability of a risk occurring from all sources and categories. We have then developed a list of the policies which could be employed to mitigate the risks and seek estimates of the effect on the overall incidental risk emanating from each source that each policy might be expected to have. We then calculate the overall residual risk that remains once these mitigating effects have been taken into account.

Figure 1 provides a visualisation of the model we have developed for empirical estimation of incidental risks.

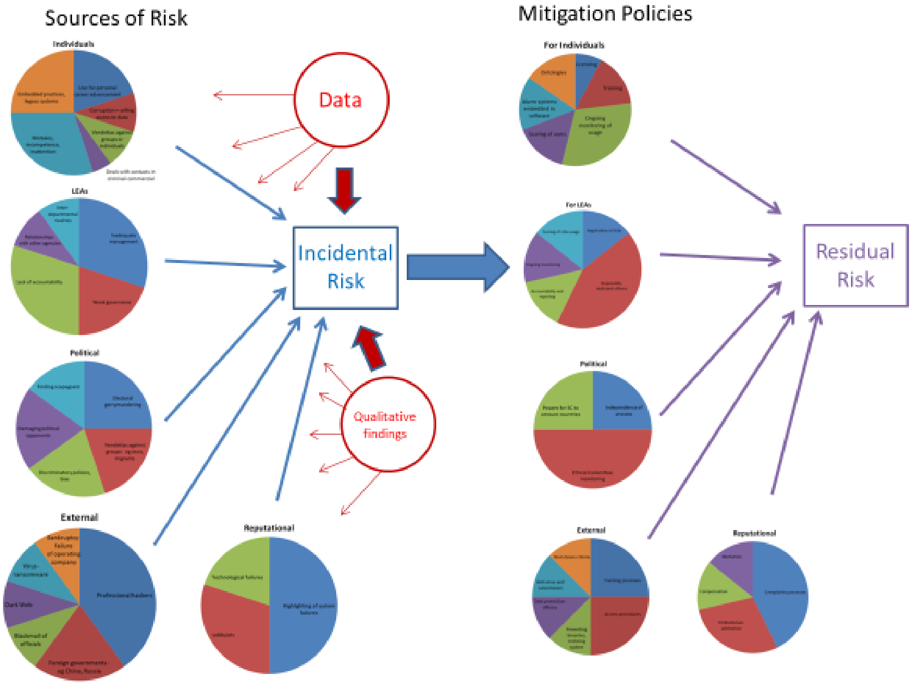

Figure 1. SPIRIT Incidental Risk Estimation Model

Refinement of the probability estimates which lead to this estimate is the subject of ongoing work within the SPIRIT project. Obviously, the objective of the policies is to create zero residual risk, and our work is intended to validate the probability and impact estimates, to permit mitigation policies to be refined so that this outcome – or something very close to it - is achieved.

4.2. Further risk mitigation

Within the SPIRIT Project we distinguish between (i) incidental findings that may occur during research, and (ii) incidental findings that may occur in the use of the technology by LEAs.

With regard to the former category, SPIRIT carries out research which uses both *ad hoc* data and anonymised data provided by LEAs. When using such data there may be the possibility of reconstructing the information to identify a real person thus incurring in re-identification. We have developed testing procedures which ensure that no real person can be identified from the data used for our research, or if a person is identified that they will be notified, and their data erased from the relevant datasets.

In the development phase of SPIRIT, human intervention points are being built into algorithms, methods and crawlers so that, when used, it will provide transparent levels of authority to progress the investigation into open source data or closed data such as emails, closed social network profiles, bank records, etc.

5. Data Protection by design (DPbD): An Indirect Strategy

5.1. Indirect strategy

Our work for SPIRIT includes the development of an action plan to mitigate the identified risks related to identity. It can be broadly summarised as follows:

- Defining the information flow in advance for all functionalities of the platform.
- Embedding alerts and protections into the architecture to detect breaches and accidents as soon as possible, identifying the information flow in which the breach has been produced.
- Defining and identifying ethical and legal requirements to be modelled, according to (i) hard law (national and EU regulations, GDPR, Directive 2016/680/EU), (ii) EU Data Protection Supervisor and national policies and Data Protection Authorities, (iii) soft law (protocols, standards), (iv) ethical expertise.
- Introducing a quick communication system between researchers, LEAs, SPIRIT DPO, and the members of the EAB.
- Redefining the algorithms and identity conceptual models (entities, attributes, relationships) if required.
- Setting up the SPIRIT Regulatory Model (SRM) to monitor all milestones and stages of development.
- Defining the ethical rules following the legal requirements coming from the European, national and regional legislation and guidelines of Art 29 Working Party.
- Setting a privacy ontology model seeking for (i) interoperability, (ii) embedding privacy protections into the system, reusing some parts of the ongoing general GDPR ontology.
- Integrating (i) anonymization, (ii) encryption, (iii) privacy preserving algorithm developments, (iv) and authorisations, into SRM.

- Reassuring that all LEAs that participate in the project will receive the SPIRIT guidelines to use the platform according to the SPIRIT Regulatory Model. Including in the dissemination plan strategies to communicate the project to, whenever possible, a general audience, in order to create an opportunity for dialogue on potential concerns about the balance between, on the one hand, the need to develop new technologies for fighting crime and terrorism and, on the other hand, the protection of citizens' fundamental rights.

Figure 2 illustrates this indirect strategy to implement Data Privacy by Design (DPbD) [2] [3]. General Data Protection Principles have been turned into specific modelling actions: (i) enforce, (ii) demonstrate, (iii) control, (iv) inform, (v) minimise, (vi) abstract, (vii) separate, (viii) and hide. External and internal controls have been set for: (i) Data access, (ii) Data collection, (iii) Data reuse and transfer, (iv) Data protection controls.

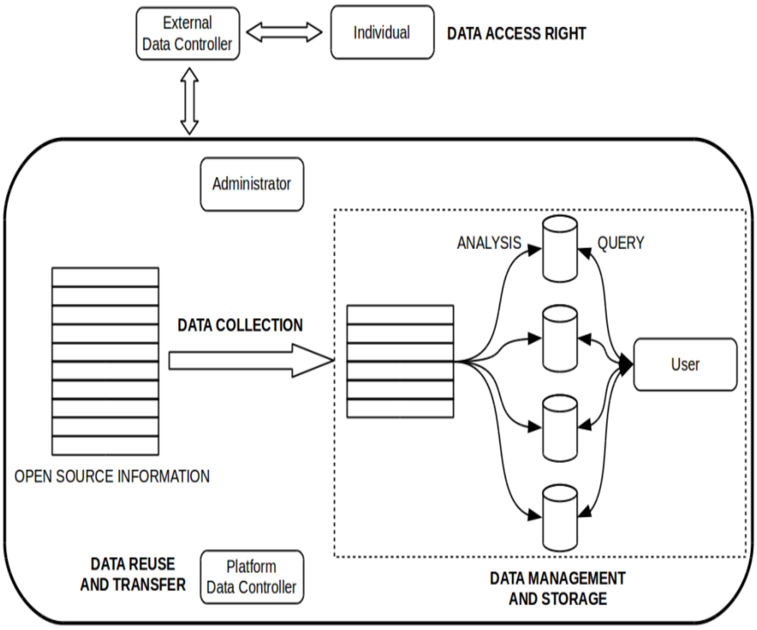

Figure 2. SPIRIT Indirect strategy embedding data protection controls [3] [9].

5.2. Identity and legal compliance

Anonymisation of the data reduces the value of the data to investigators, and de-anonymisation seems to be possible in many cases, which limits the value of this as a privacy-protection mechanism. Different degrees of pseudonymisation are possible, and different methods will have different effects both on usability and on the ease with which de-anonymisation can be achieved.

In the broad sense, we seek to find methods whereby those who use the SPIRIT system comply with relevant legal, regulatory, social and ethical requirements in doing so. This includes only using the system for the specific purposes for which it is authorised, and not using it for other purposes.

A variety of risks have been identified in previous work, including risks related to: (i) the lawfulness of processing, (ii) specification of purpose, (iii) breaches of the data minimisation principle, (iv) inaccuracy of data, (v) data storage and retention, (vi) data security, (vii) access rights, (viii) information rights, (x) accountability and monitoring.

6. The Spirit Regulatory Model (SRM)

6.1. Hard law: license system

Risk mitigation procedures are being developed to counter these risks, some of which involve technological or physical measures. But many of the risks relate to non-authorised or/and even inappropriate use of the data by individuals within the law enforcement agencies, or by the leadership of those agencies. These are harder to mitigate through rules, penalties etc. So, we could develop a methodology whereby the system is only used by those deemed to be trustworthy. Individual and collective agents should be carefully distinguished here, as the regulation, evaluation, and monitoring of LEAs is one of the competencies of national-states.

One possibility is using a hard law approach. In addition to a regular incidental findings policy, a licensing system could be developed for the use of the system, which could include features such as (i) psychological, past convictions, misdemeanours or unethical screening of individuals, and (ii) organisation scoring according to past breach of regulations or unethical behaviour. If an organisation's score falls below a pre-determined level, access to the system could be withdrawn, pending an investigation, to be granted again only if relevant safeguards, retraining etc. have been introduced.

We can also identify the requirements for each type of law enforcement activity for which the system might be used. Some would require less intensive/intrusive investigation than others. So it may be helpful to develop the SPIRIT system to provide different levels of information, for example with more or less anonymization. If this is done, the suitability scores required to be granted access to each level of the system could be set at different levels.

6.2. Legal governance: The Spirit Regulatory Model

A second possibility which is not incompatible with the first one is following the path of EU better or smart regulations for legal governance [12] while protecting fundamental rights.[13] This is based on fostering *organisational trust*, and it is a less intrusive and drastic way of monitoring. I.e. (i) the final evaluation is shared by multiple

[12] https://ec.europa.eu/commission/priorities/digital-single-market_en

[13] https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights_en

bodies (including independent ethical Committees at EU level, EU and national Data Protection Offices, and international and national judicial authorisations and iterative permits); and (ii) LEA officers and investigators can be provided with training courses on the protections set by the EU recent provisions.

To monitor the overall data acquisition and use processes a SPIRIT Regulatory Model is being developed, plotting, mapping and following all information processes that will take place on the platform (Fig. 3). The model will in due course include all regulatory sources (hard law, soft law, policies and ethics) endorsed, as said, as smart (or better) regulations by the EU strategy to embed protections into computational systems. This strategy was first tested in previous EU security projects [3] [9]. Data collected and processed will not be held or further used unless this is essential for reasons that are clearly stated in advance to support data protection. The model will integrate computational measures (e.g. ontologies) with data management and organisation.

SPIRIT includes the following capabilities and technical elements which are being developed: (i) Data Acquisition and Extraction: Semantic capabilities, Dark web capabilities, Online social network capabilities, multi-purpose semantic crawler; (ii) Social Graph Construction: Text analytics and mining, speech and audio analytics and mining, video and image analytics and mining, social graph modelling; (iii) Graph Infrastructure and Analysis: knowledge management and graph analysis, data processing systems; (iv) Scalable & Secure Distributed Processing & Integration: security and data protection measures, security evaluation, security semantics; (v) Identity Sense-Making Workspace: search and retrieval, data exploration, semantically supported data manipulation interactivity, automated data mining tools, cognitive support, collaboration.

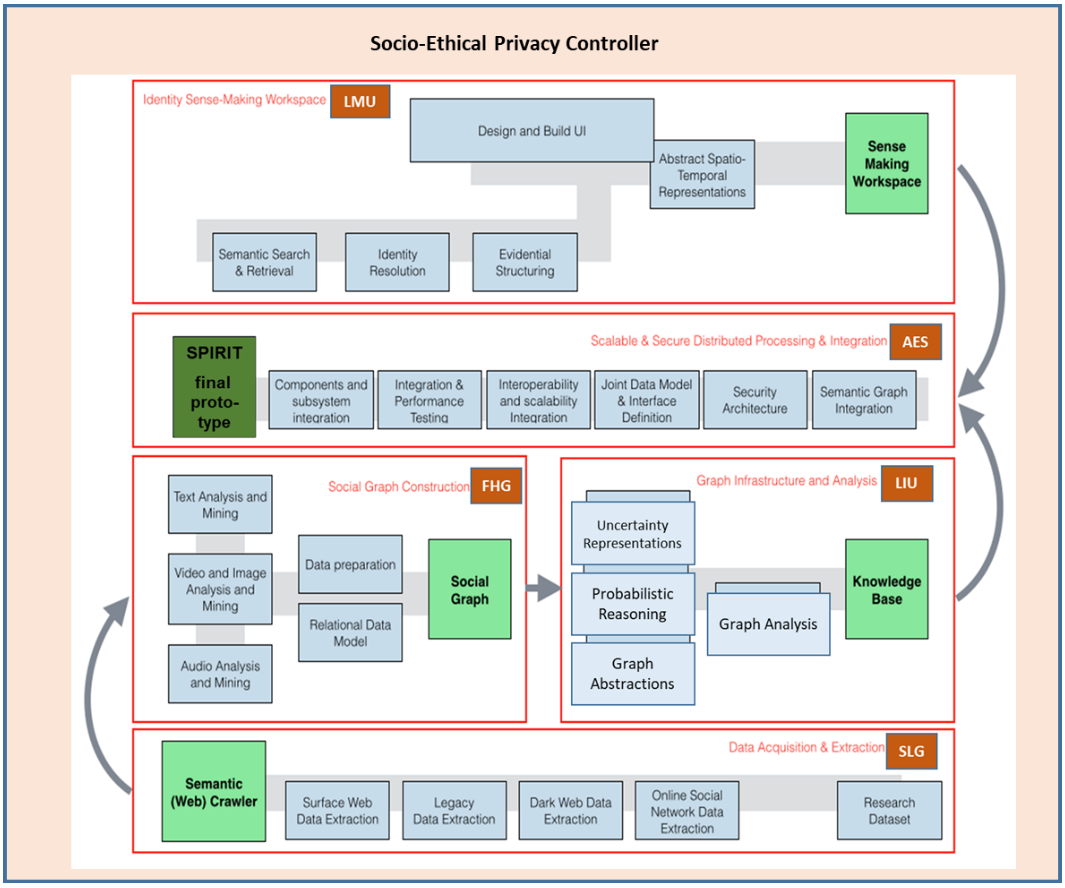
Socio-Ethical Privacy Controller
Identity Sense-Making Workspace
LMU
Design and Build UI
Abstract Spatio-Temporal Representations
Sense Making Workspace
Semantic Search & Retrieval
Identity Resolution
Evidential Structuring
Scalable & Secure Distributed Processing & Integration
AES
SPIRIT final proto-type
Components and subsystem integration
Integration & Performance Testing
Interoperability and scalability Integration
Joint Data Model & Interface Definition
Security Architecture
Semantic Graph Integration
Social Graph Construction
FHG
Text Analysis and Mining
Video and Image Analysis and Mining
Audio Analysis and Mining
Data preparation
Relational Data Model
Social Graph
Graph Infrastructure and Analysis
LIU
Uncertainty Representations
Probabilistic Reasoning
Graph Abstractions
Graph Analysis
Knowledge Base
Data Acquisition & Extraction
SLG
Semantic (Web) Crawler
Surface Web Data Extraction
Legacy Data Extraction
Dark Web Data Extraction
Online Social Network Data Extraction
Research Dataset

Fig. 3 - SPIRIT System Architecture: Main Architectural Components

7. Final remarks and future work

SPIRIT is a complex project for security compliance. It is complex from technical, ethical, and legal points of view. It should be effectively and alternatively tested by six police units of five different countries (UK, Belgium, Greece, Poland and Serbia). It should furnish a set of reliable tools to track identities in the dark web. And it should endorse at the same time the protections of rights of many national and European legislations. Not all jurisdictions present the same type of requirements.

The GDPR came into force in May 25th 2018. SPIRIT officially started in August 1st of the same year. It had to obtain the approval first of many Ethical Committees, and to respond twice to no less than 27 ethical and legal questions raised by the EU Commission. The SPIRIT Ethical Advisory Board was officially launched in August 29th, prior to the official kick-off of the project, and has been really busy since then.

All real data must be anonymised and made accessible only for the police officers. Researchers are put aside and walkthroughs and tests must be conducted separately. Internal protections are so strong that will include police screening tests, interviews, focus groups and scores that have been unusual in this type of research until now. In addition to privacy ontologies, information flowcharts have been set in advance to foresee possible breaches, prevent de-identification, and redress privacy conflicts. A DPIA was also conducted and it will evolve all along the project.

For all these reasons, SPIRIT is a kind of benchmark for the implementation of DGPR provisions in the area of security. This paper is the first step in keeping track of the solutions that could be implemented.

These solutions should not raise more hurdles for the police work in organised crime and terrorism investigations, and should be effectively protective of citizens' rights, preventing discrimination against vulnerable social groups.

Complying with all requirements and objectives at the same time is not trivial. One of the main proposals has been to turn up the incidental findings policies that were coined and raised in bioethics, genetics and FRMI studies some years ago into an effective policy of incidental risks. This has allowed us to figure out and apply metrics instead of ticking boxes on a list.

Acknowledgements

This research is funded by SPIRIT. Scalable privacy preserving intelligence analysis for resolving identities. European Commission. Contract 786993. Views expressed herein are however not necessarily representative of the views held by the funders.

References

[1] Article 29 Working Party, Guidelines on consent under Regulation 2016/679, WP 259, 1st 28 November 2017. Available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=62305 1

[2] Casanovas, P. Cyber Warfare and Organised Crime. A Regulatory Model and Meta-Model for Open Source Intelligence (OSINT). In R. Taddeo and L. Gkorioso, Ethics and Policies for Cyber Operations, pp. 139-167: Dordrecht: Springer International Publishing (2017)

[3] Casanovas, P., Arraiza, J., Melero, F., González-Conejero, J., Molcho, G., & Cuadros, M. Fighting Organized Crime through Open Source Intelligence: Regulatory Strategies of the CAPER Project. Proceedings of the 27th annual conference on Legal Knowledge and Information Systems, JURIX-2014, pp.189-199, Amsterdam, IOS Press (2014)

[4] Damjanovicova, M. Incidental Findings. In Ethical Counselling and Medical Decision-Making in the Era of Personalised Medicine (pp. 89-95). Springer, Cham (2016)

[5] Erdmann, P. Incidental Findings–Ethical Aspects. In Incidental Radiological Findings (pp. 9-24). Springer, Cham (2016)

[6] EU Regulation (EU) 2016/679 of the European Parliament and of the Council 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, and repealing Directive 95/46/EC (General Data Protection Regulation) https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

[7] EU Directive (EU) 2016/680 of the European Parliament and of the Council 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, and repealing Council Framework Decision 2008/977/JHA. http://data.europa.eu/eli/dir/2016/680/oj

[8] EU Committee of Ministers. Recommendation CM/Rec (2017) 6 of the Committee of Ministers to member States on “special investigation techniques” in relation to serious crimes including acts of terrorism (Adopted by the Committee of Ministers on 5 July 2017 at the 1291 st meeting of the Ministers' Deputies. https://rm.coe.int/1680730408

[9] González-Conejero, J., Figueroa, R.V., Muñoz-Gomez, J. and Teodoro, E., Organized crime structure modelling for European Law Enforcement Agencies interoperability through ontologies. In AI approaches to the complexity of legal systems (pp. 217-231). LNAI 8929, Springer, Berlin, Heidelberg (2014)

[10] Havinga, H.N.J. and Sessink, O.D.T. Risk Reduction Overview. In International Conference on Availability, Reliability, and Security , in S. Teufel et al. (Eds.), CD-ARES 2014, LNCS 8708, Springer: Cham, pp. 239-249 (2014)

[11] Schmücker, R., Incidental Findings: Definition of the Concept. In: Weckbach S. (eds) Incidental Radiological Findings. Medical Radiology. Springer, Cham, pp. 3-7 (2016)

[12] Young W., and Nancy Leveson. N. Systems thinking for safety and security. In Proceedings of the 29th Annual Computer Security Applications Conference (ACSAC '13). ACM, New York, NY, USA, 1-8 (2013)

[13] Wolf, S.M, Lawrenz F.P, Nelson C.A, et al. Managing Incidental Findings in Human Subjects Research: Analysis and Recommendations. J Law, Med Ethics. 36 (2): 219–248. doi:10.1111/j.1748-720X.2008.00266.x. (2008)