Information & Security

Published since 1998

J. Rajamäki, vol. 43, no. 2 (2019): 196-214
https://doi.org/10.11610/isij.4316

ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

Design Science Research towards Privacy by Design in Maritime Surveillance ICT Systems

Jyri Rajamäki

Laurea University of Applied Sciences, https://www.laurea.fi/en/

ABSTRACT:

Maritime surveillance is essential for creating maritime awareness. When open source intelligence (OSINT) is becoming a part of it, privacy in surveillance will be a special concern. However, processing of personal data in surveillance is regulated by the General Data Protection Regulation (GDPR) and/or by the Directive 2016/680 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. In both of these regulations, Privacy by Design (PbD) approach is mandatory. GDPR encourages applying a Data Protection Impact Assessment (DPIA) to identify and minimize data protection risks as the initial step of any new project. This design science research shows how PbD and DPIA are adapted in the MARISA project and tries to be a step towards new meta-artefacts and useful methods for the design and validation of privacy requirements engineering approaches into maritime surveillance ICT systems.

ARTICLE INFO:

RECEIVED: 08 MAY 2019

REVISED: 28 AUG 2019

ONLINE: 21 SEP 2019

KEYWORDS:

maritime surveillance, privacy, GDPR Directive, open source intelligence, OSINT, impact assessment

Introduction

The ongoing MARitime Integrated Surveillance Awareness (MARISA) project[2] funded by the Horizon 2020 programme, focuses on four major objectives: 1) cre-

✉ E-mail: jyri.rajamaki@laurea.fi

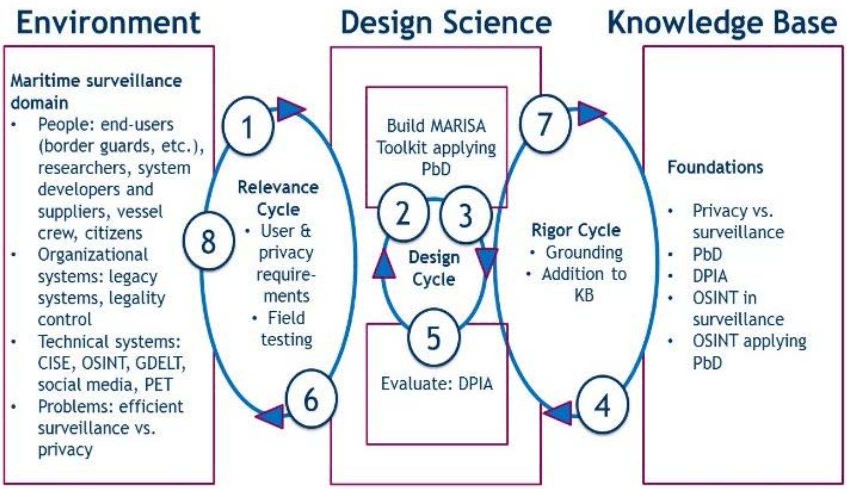
ate improved situational awareness with a focus on delivering a complete and useful comprehension of the situation at sea; 2) support the practitioners along the complete lifecycle of situations at sea, from the observation of elements in the environment up to detection of anomalies and aids to planning; 3) ease a fruitful collaboration among adjacent and cross-border agencies operating in the maritime surveillance sphere (Navies, Coast Guards, Customs, Border Polices) in order to pull resources towards the same goal, leading to cost efficient usage of existing resources; and 4) foster a dynamic eco-system of users and providers, allowing new data fusion services, based on a "distilled" knowledge, to be delivered to different actors at sea by the integration of a wide range of data and sensors.

The General Data Protection Regulation (GDPR) and the Directive 2016/680 "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" regulate processing of personal data also as a part of the maritime surveillance. Privacy by Design (PbD) is one of the key requirements in the European Data Protection Reform and it is included in GDPR and Directive 2016/680. To satisfy its requirement, GDPR encourages organizations to undertake a Data Protection Impact Assessment (DPIA) to identify and minimize data protection risks as the initial step of any new project. This means that PbD and DPIA are mandatory requirements in MARISA context. Although PbD and DPIA as concepts are becoming well-known, it turns out that there is not much standardization in how to actually apply them. This paper presents how PbD and DPIA are adapted in the MARISA project and tries to be a step towards new meta-artefacts and useful methods for the design and validation of privacy requirements engineering approaches into maritime surveillance ICT systems.

In contrast to behavioural science, design science research (DSR) aims to provide four general outputs: (1) constructs, (2) models, (3) methods, and (4) instantiations.[3] Fig. 1 shows how the DSR framework is applied and how the DSR checklist [1] questions are mapped in this paper. After this introduction, section 2 presents the maritime surveillance environment. Section 3 deals with the present knowledge base with regard to (1) privacy by design, (2) data protection impact assessments, (3) applying open source intelligence (OSINT) in law enforcement, and (4) PbD in OSINT. Section 4 presents how PbD is adopted in building of the MARISA Toolkit and section 5 how this is evaluated. Finally, section 6 answers to the DSR checklist questions and concludes the paper.

Environment

The Maritime Common Information Sharing Environment (CISE) seeks to further enhance and promote relevant information sharing between authorities involved in maritime surveillance from coastguards and navies to port authorities, fisheries controls, customs authorities and environment monitoring and control bodies. The EUCISE2020 project [4] has taken the level of collaboration forward, in putting operational authorities together at an unprecedented scale to define the largest


Environment
Design Science
Knowledge Base
Maritime surveillance domain
• People: end-users (border guards, etc.), researchers, system developers and suppliers, vessel crew, citizens
• Organizational systems: legacy systems, legality control
• Technical systems: CISE, OSINT, GDELT, social media, PET
• Problems: efficient surveillance vs. privacy
1
8
6
Relevance Cycle
• User & privacy require-ments
• Field testing
Build MARISA Toolkit applying PbD
2
3
Design Cycle
5
Evaluate: DPIA
7
4
Rigor Cycle
• Grounding
• Addition to KB
Foundations
• Privacy vs. surveillance
• PbD
• DPIA
• OSINT in surveillance
• OSINT applying PbD

Design science research checklist questions:
(1) What is the research question (design requirements)?
(2) What is the artefact? How is the artefact represented?
(3) What design processes (search heuristics) will be used to build the artefact?
(4) How are the artefact and the design processes grounded by the knowledge base? What, if any, theories support the artefact design and the design process?
(5) What evaluations are performed during the internal design cycles? What design improvements are identified during each design cycle?
(6) How is the artefact introduced into the application environment and how is it field tested? What metrics are used to demonstrate artefact utility and improvement over previous artefacts?
(7) What new knowledge is added to the knowledge base and in what form (e.g., peer-reviewed literature, meta-artefacts, new theory, new method)?
(8) Has the research question been satisfactorily addressed?

Figure 1: Design Science Research framework of the study (modified from [1]).

European test bed for data and information exchange. DG MARE Test Project CoopP on cooperation in execution of various maritime functionalities at sub-regional or sea-basin level in the field of integrated maritime surveillance has investigated information exchange needs, barriers, benefits and technologies by analysing use cases, agreed at the level of large user community.

The MARISA project fosters faster detection of new events, better informed decision making and achievement of a joint understanding of a situation across borders and allowing seamless cooperation between operating authorities and on-site / at sea / in air intervention forces. Its solution is a toolkit that provides a suite of services to correlate and fuse various heterogeneous and homogeneous data and information from different sources, including Internet and social networks.

The project also aims to build on the huge opportunity that comes from using the open access to "big data" for maritime surveillance: the availability of large to very large amounts of data, acquired from various sources ranging from sensors, satellites, open source, internal sources and of extracting from these amounts through advanced correlation improves knowledge.

The MARISA Toolkit provides new means for the exploitation of the bulky information silos data, leveraging on the fusion of heterogeneous sector data and taking benefit of a seamless interoperability with the existing legacy solutions available across Europe. In this regard, the data model and services specified in the EU-CISE2020 project.[4] will be exploited, combining with the expertise of consortium members in creating security intelligence knowledge from a wide variety of sources.

Level 1 addresses the aspect of "Observation of elements in the environment" to build and enrich a Maritime Situation Awareness (MSA). The main focus is on establishing enhanced information about the geographical position of the observed objects providing Data Fusion services, such as "Multi Sensor/ Target/ Common Operating Picture (COP) Fusion," "Object Clustering," "Maritime route extraction," "Density maps," and "Multilingual Information Extraction and Fusion from social media." Level 2 addresses the aspect of "Comprehension of the current situation" to provide useful information among the relationships of objects in the maritime environment. The goal is to detect suspicious behaviour of maritime entity (particular and irregular patterns) and infer the real vessel identity (fishing, polluting, smuggling) providing Data Fusion services, such as "Business Intelligence," "On-Demand Activity Detection," "Behaviour Analysis," "Anomaly Detection & Classification," and "Alarm Generation." Level 3 addresses the aspect of "Projection of future states" to predict the evolution of a maritime situation, in support of rapid decision making and action. The focus is on predicting future behaviour (time, place and probability of type of activity) and mission planning support based on predicted behaviour of vessels in the region of interest providing Data Fusion services, such as "Predictive Analysis" and "Mission Planning."[5]

The "MARISA User Application" level includes all the computing facilities to let MARISA End Users to visualize results of the MARISA services in a set of different graphical and statistical presentations, based on a Web Based approach. For each end user community of interest (generic, data fusion expert and MSA operators) different representation of MARISA Data Fusion Products will be made available, based on access privileges assigned to them. MSA Presentation Web Console enables generic user to access, analyse and visualize maritime entities in textual (dashboard) or graphical views, using a Web browser as a client. The situational awareness of the maritime domain will be provided through a fused maritime picture based on a WebGIS and reference detailed cartographic map of a selected Area of Interest (AoI). This service also includes the capability to monitor the Maritime Situation to detect abnormal behaviour and highlight alarms. Data Fusion Expert Console addresses the aspect of "Man in the loop" as defined in MARISA Level 4 services. Data Fusion experts will be able to have a range of interactive content types available, in order to refine data sources and data fusion products coming from MARISA processing. A web-based application approach will be pursued. System Administration Console will be primary devoted to address the general management activities of the MARISA system. The console will also be used to profile and assign privileges to generic end users and operational systems when accessing data fusion and HCI services.[5]

The "MARISA Networking and Integration Services" level includes computing components. Access Control Services manage the access to MARISA Data Fusion products and deal with the ability of MARISA to identify, record and manage users' identities and their related access to all the services made available by the toolkit. They include a) Identity and Access management services to identify all the users connecting to the toolkit's services and to assure that access privileges are granted according to defined security policies, and all individuals and systems are properly authenticated, authorized and audited, b) User Profiling service record and assign privileges to all users (human/device/process) connecting to MARISA. Data Source Interfaces (I/F) Services gather data, information and services from external sources, such as End User Legacy Systems & Assets, Free & Open Internet Sources, Simulation Sources as well as some assets directly provided by MARISA such as Satellite Data, Signal Analysis Devices, Automatic Identification System (AIS) Sources. The sources feeding the MARISA Toolkit are expected to be: Maritime data (e.g. AIS Network, System Tracks, Mission Plans, etc.); Satellite data (e.g., COSMO-SkyMed SAR data, Sentinel-1, Sentinel-2, commercial optical missions, etc.); Intelligence data (e.g., OSINT, Signal Analysis).[5]

Knowledge Base

As Hevner and Chatterjee state,[1] design science draws from a vast knowledge base of scientific theories and engineering methods that provides the foundations for rigorous DSR. This section defines the state of the art in the application domain of the research, which is privacy in surveillance. First, we discuss how to attune surveillance and privacy. Then, we look privacy engineering in general: privacy by design approach (PbD), and how the success of this approach can be evaluated by a data protection impact assessment (DPIA). Finally, we focus to the usage of social media in surveillance that has been rated to be the biggest privacy challenge during the use of the MARISA Toolkit [6] and how to apply PbD approach in open source intelligence.

Privacy, Surveillance and Privacy by Design

New surveillance technologies became omnipresent in our everyday live. While early research focused on functionality of these technologies, e.g. face recognition or violence detection, latterly also privacy and transparency related work has been made.[7] While this research helps us to design systems that combine functionality and privacy, only little understanding is present how the people under surveillance will react to the new systems; average citizens do not understand technological details and they are unable to distinguish between systems with varying privacy protection.[7] Privacy in surveillance is a special concern when, for example, using drones and surveillance cameras, with automated border control, and when collecting and analysing big data. In addition, the impact of new surveillance technologies on the fundamental rights of asylum seekers and refugees as well as the increased responsibility this more effective situational awareness brings (under international refugee law and the Search and Rescue regime: duty to render assistance) have all been debated by numerous scholars.[8] Surveillance has a bad reputation in most countries. Many surveys for understanding the acceptance of surveillance were made in special places (airports, public transport and shopping malls), but their outcome depends on recently happened events, e.g., a terrorist attack or a reported misuse of a video sequence and the underlying factors are not considered and no generic model for the acceptance exists.[7]

Privacy by design (PbD) is an approach to systems engineering approach intended to ensure privacy protection from the earliest stages of a project and to be taken into account throughout the whole engineering process. The PbD concept is closely related to the concept of privacy enhancing technologies (PET) published in 1995.[9] PbD framework was published in 2009.[10] The concept is an example of value sensitive design that takes human values into account in a well-defined manner throughout the whole process. PbD is one of the key requirements in the European Data Protection Reform beings included in the General Data Protection Regulation (GDPR) and Directive 2016/680. The GDPR also requires Privacy by Default, meaning that the strictest privacy settings should be the default.

Data Protection Impact Assessment

To satisfy its requirement, GDPR encourages organizations to undertake a Data Protection Impact Assessment (DPIA) to identify and minimize data protection risks as the initial step of any new project. DPIA is a process designed to describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them.[11] DPIAs are important tools for accountability, as they help controllers not only to comply with requirements of the GDPR, but also to demonstrate that appropriate measures have been taken to ensure compliance with the Regulation. In other words, a DPIA is a process for building and demonstrating compliance.[11] DPIAs should be relatively cheap to implement with sufficient resources and tools.[12] However, while there is advice on the legal requirements for DPIA and the elements of what practitioners should do to undertake a DPIA there has been little prescription about how security and privacy requirements engineering processes map to the necessary activities of a DPIA, and how these activities can be tool-supported.[12]

Coles, Fairy and Ki-Aries have studied existing privacy requirements engineering approaches and tools that support carrying out DPIAs.[12] The existing approaches capture the elements that would be needed by a DPIA, but two barriers need to be overcome before such approaches are ready for security and practitioners to use in DPIAs:[12] 1) more prescription is needed to indicate what tools and techniques map to different stages of a DPIA, and 2) such steps need to be adequately tool-supported, such that data input in one step can be used to support reasoning and analysis in others. Their main contributions:[12] 1) existing Requirements Engineering techniques associated with Integrating Requirements and Information Security process framework can be effective when supporting the different steps needed when carrying out a DPIA, but there is no one-to-one mapping between requirements and techniques, and several techniques might be needed to support a single step; 2) demonstration how an exemplar for Security Requirements Engineering tools supports and helps reason about potential GDPR compliance issues as a design evolves; and 3) they present a real example where their approach assessed the conceptual design of a medical application without an initial specification, and only the most preliminary of known functionality. They show that the use of this approach and the Requirements Engineering techniques in general, are effective in discovering additional functionality, and envisaging different forms of intended and unintended device use.[12]

OSINT and Surveillance

OSINT is intelligence collected from publicly available sources, including the internet, newspapers, radio, television, government reports and professional and academic literature.[13] OSINT binds through a systematic analysis process as a tight and informative thematic entity, the scattered information to be obtained from open sources. During the last few years, the internet and especially social media channels have revolutionized the ones that had significantly increased the amount of OSINT and information to be analysed.[8] OSINT requires knowledge of the network environment with a good performer, a comprehensive means selection and problem-solving skills. Ethical questions apply to the handling of the collected information. When collecting data from people, one must remember that the creation of person registers is strictly regulated.[8]

On the market there are numerous efficient network analysis tools, some of which are also used by the LEAs. Wells and Gibson have studied OSINT from a UK perspective and considered the law enforcement and military domains.[14] Their conclusion was that the UK police and military open source investigations have a great number of similarities. However, there are several observable differences: (1) the handling of a chain of evidence; police forces prioritize and integrate a chain of custody for any intelligence that may lead to prosecution in a court of law and therefore the police tend to have a more structured and detailed approach to evidence gathering; (2) the use of third party software and developers; the military prioritizes the use of bespoke software tools and in-house training solutions, where the police have rationally used a variety of commercial and private sector solutions, some of which are specifically designed for police OSIN; and (3) the approach towards the dark web; the military has a far more cautious approach to operating on the dark web, whereas the police have faced both pressure and a necessity to operate in this domain due to policing-specific concerns, such as online child sexual exploitation.[14]

The International and EU regulation of OSINT includes the regulations and conventions. However, even though international regulatory guidelines are available, specific allowances, prohibitions and exceptions mainly stem from national legislation.[15] Koops presents procedural issues of OSINT in police investigations and investigates criminal-procedure law in relation to open source data gathering by the police.[16] He studies the international legal context for gathering data from openly accessible and semi-open sources, including the issue of cross-border gathering of data. This analysis is used to determine if investigating open sources by the police in the Netherlands is allowed on the basis of the general task description of the police, or whether a specific legal basis and appropriate authorization is required for such systematic observation or intelligence. The European Data Protection Reform partly harmonizes the general data protection regulation in EU countries (General Data Protection Regulation), but in the case of law enforcement and crime prevention it still offers variation in the national level legislation (Data Protection Directive). Hu identifies five key related concerns.[17] The first question in relation to open sources is the following: How trustworthy are they? Also, the line between espionage and OSINT can be very thin, therefore caution and double-checking are advised before conducting OSINT activities.[18] Koops [16] also underlines the need for OSINT tools to meet non-manipulability and auditing requirements associated with digital forensic quality assurance.

PbD and OSINT

Koops, Hoepman and Leenes consider the challenge of embedding PbD in OSINT carried out by law enforcement.[15] Ideally, the technical development process of OSINT tools is combined with legal and ethical safeguards in such a way that the resulting products have a legally compliant design, are acceptable within society (social embedding), and at the same time meet in a sufficiently flexible way the varying requirements of different end-user groups. Koops, Hoepman and Leenes use the analytic PbD framework and they discuss two promising approaches, revocable privacy and policy enforcement language.[15] The approaches are tested against three requirements that seem suitable for a "compliance by design" approach in OSINT: purpose specification; collection and use limitation and data minimization; and data quality (up-to-datedness).[15] For each requirement, they analyse whether and to what extent the approach could work to build in the requirement in the system. They demonstrates that even though not all legal requirements can be embedded fully in OSINT systems, it is possible to embed functionalities that facilitate compliance in allowing end-users to determine to what extent they adopt a "privacy by design" approach when procuring an OSINT platform, extending it with plug-ins, and fine-tuning it to their needs. Therefore, developers of OSINT platforms and networks have a responsibility to make sure that end-users are enabled to use PbD, by allowing functionalities such as revocable privacy and a policy enforcement language.[15] Even though actual end-users have a responsibility of their own for ethical and legal compliance, it is important to recognize that it is questionable whether all responsibility for a proper functioning and use of OSINT platforms can be ascribed to the end-users; and some responsibility for a proper functioning of OSINT framework in practice also lies with the developers of the platform and individual components.[19]

Privacy as for the Overall Design

Necessary Distinction: Research vs. End-use

In view of the privacy requirements, it is essential to clarify two relevant aspects: 1) the development of the MARISA Toolkit by the research consortium and, 2) (possible) end-use of this toolkit by relevant authorities. This distinction is important, as different legal and ethical standards may apply. An example can be given from the domain of data protection legislation. The European Commission put forward its EU Data Protection Reform in 2012 to make Europe fit for the digital age and it includes two parts, which are both relevant in the MARISA context: 1) 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, GDPR); 2) 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.

There are differences between the regulation and the directive especially in the principles and lawfulness of the personal data processing and on the rights of the data subject. However, the responsibilities of register owners and data processors are quite similar. In addition, the nature of the directive is different: The Act/Regulation (GDPR) is applicable as such in each EU country, whereas the Directive 2016/680 has to be transposed in to national law. Directive 2016/680 shall not preclude Member States from providing higher safeguards than those established in Directive 2016/680 for the protection of the rights and freedoms of the data subject with regard to the processing of personal data by competent authorities, and so national laws may differ in Member States. Since MARISA is designed both for criminal prevention, and for other activities, like Search and Rescue (SaR), we will take both documents as a starting point of this investigation.

Regulation applies always when personal data processing takes place in the EU relating to the operations of establishment based in there. This will apply regardless of whether the actual processing takes place in the EU. Regulation will also apply when the controller organization is based outside the EU, but the individuals the processing concerns, are EU citizens and processing is about offering goods or services to them or monitoring their behaviour. In GDPR, this is referred as “territorial scope.” (The regulation will not be applied solely on the use of personal or private data.) The regulation is applied always when personal data is processed wholly or partly by automated means. Regulation also applies when the data is not processed by automated means but forms a part, or is intended to form, a part of a filing system. In GDPR, this is referred as “material scope.”

Behind the Directive 2016/680 there is also the need for data exchange: As stated in the Directive 2016/680: "The free flow of personal data between competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security within the Union and the transfer of such personal data to third countries and international organizations, should be facilitated while ensuring a high level of protection of personal data."

Both GDPR and Directive 2016/680 have their ground in the European Convention on Human Rights and on the EU Fundamental Rights. It is important to remember that the main goal of GDPR is not to deny the processing of personal information. The goal of regulation is to add transparency and highlight the responsible processing of personal data.

GDPR is applicable to the researchers of the whole MARISA project involved with the processing of personal data. The development of the MARISA Toolkit including trials of the prototype is aimed at proving functionality and is carried out by public and private parties. The MARISA consortium consists of a selection of twenty-two partners, representing leading European organizations from large enterprise, small and medium enterprise, academia, non-profit organization and end users. Even though MARISA is a research project and as such not directly aimed at exploitation of the research results, the prototype is developed in view of possible end-use by various aspects of maritime surveillance: marine environment, fisheries control, maritime safety, defence, border control, customs, and general law enforcement. In this respect, Directive 2016/680 is effective regarding the processing of personal data in the domain of police and judicial cooperation in criminal matters and during the end-use of MARISA toolkit, both GDPR and Directive 2016/680 are applicable. Even though GDPR and Directive 2016/680 are similar, important differences relate to specific exceptions and legitimate processing grounds that are reserved for public authorities in the field of law enforcement and intelligence, creating more leeway for them than is the case regarding private parties.

Because of differences in applicable legal regimes, it is necessary to perform similar two-tiered legal and ethical analysis within the MARISA project as was made during the VIRTUOSO project.[19] On the one hand the legal assessment of the prototype, as embodiment of the MARISA Toolkit and relevant components. In demonstrating MARISA functionality, the researchers involved needed to perform acts with legal implications, such as the processing of personal and/or copyright protected data.

Privacy-by-Design in MARISA Toolkit

The implementation of privacy-by-design in the MARISA Toolkit is an overall requirement or constraint for the development of the whole MARISA project.[6] MARISA architectural concept and operational environment is earlier described in Section 2.

The MARISA Toolkit has two relevant data sources: 1) data coming from the sensors, and 2) data coming from OSINT/ Social Media. *Data from Sensors:* These sensors are embodied in the operational environment of the Legacy Systems. In these environments, owned by Participating Member State governmental entities, we can suppose that the data are used on the basis of need-to-know and need-to-share. Thus, the observance of the privacy of the data can be taken for granted. *Data from Open Sources*: This case is more problematic, since the origin of the data is not controlled for any public entity. Nevertheless, here there are two possibilities: 1) System performing in a classified environment (as could be the case in managing EU-Restricted data). Here the data coming from open sources enters, by means of a cross-domain exchange devices, in a highly regulated environment, where again the privacy of the data managed can be taken for granted, on the basis of need-to-know and need-to-share. 2) System performing in an unclassified environment (this will be the most common case).[6]

MARISA OSINT Environment and Services

MARISA project is organized according to a two-phase approach, where each phase foresees a complete MARISA life cycle iteration from the user requirements collection, toolkit design and development, to the validation of services through dedicated scenarios and use cases. So, the first phase will end with the validation of a subset of MARISA initial services. During the second phase, on the basis of the feedbacks collected during the previous activities, the already developed services will be revised and enhanced, whilst additional services will be included. The complete toolkit will be then validated again in the already defined operational scenarios.[5]

The first phase MARISA service description document [5] defines three open source related services: Twitter service, OSINT service and GDELT service.

MARISA Twitter service enables access to Open Source Social Media information. Twitter is used as an example of OSINT data source: Twitter users are fast at creating their content, there is an API available, there are Links, Mediadata, etc., there are the same type of language challenges like slang words, abbreviation, etc. Many publications in the field of NLP are done using Twitter. A special classifier with a language and domain dependent model will assess the relevance of the tweet in this context (domain, use case). The result will be an instance of the Risk class defined during the EUCISE2020 project [4] containing a list of assessed tweets with their relevance exposed in the attributes RiskProbability and RiskSeverity, the RiskLevel is a combination of Probability and Level.[5]

Open Source Intelligence involves the collection, analysis, and use of data from open sources for intelligence purposes. It is any unclassified information, in any medium, that is generally available to the public, even if its distribution is limited or only available upon payment. Existing open source solutions for Social Media data stream integration, in particular for Twitter, and a MARISA web crawling mechanism will be exploited in order to provide capabilities for discovering of alert of any kind of illegal activities in the maritime environment. The research on Social Media, based mainly on the ability to identify geo-located information, will allow to associate the OSINT information with more closely related to the marine environment information (e.g. Vessels, Sea Condition, Pollution Risks, ...) and then generate an improved Recognized Maritime picture. The particular technology used is such as to facilitate with little effort the integration of other sources from social media and from OSINT (e.g. GDELT, Twitter). The technology used, by opening a listening multilingual channel directly on social media and the chosen open informative sources allow to meet cross-border requirements of MARISA project and through the application of appropriate filtering process behavioural patterns based, allows integration and real-time data processing pipelines generation.[5]

The Global Database of Events, Language, and Tone (GDELT) is a CAMEO-coded dataset containing geo-located events with global coverage from 1979 to the present. The data are collected from news reports throughout the world and the dataset provides daily coverage on the events found in news reports published on that day. In 2015, datasets Mentions and Global Knowledge Graph (GKG) were added to GDELT. The Mentions table records the network trajectory of the story of each event in flight through the global media system while the GKG table expands GDELTs ability to quantify global human society beyond cataloguing physical occurrences towards actually representing all of the latent dimensions, geography, and network structure of the global news. Today, GDELT is a real time database of global human society for open research which monitors the world's broadcast, print, and web news, creating a free open platform for computing on the entire world containing three data tables: Event, Mentions and GKG while most researches are based only on the Event table.[20] MARISA GDELT service integrates open-source intelligence data from GDELT project into MARISA. It filters the results using natural language processing in order to identify possible events related to Maritime domain, such as naval incidents, piracy events, and pollution events.[5]

In any case, the data coming from sensors or open sources will enter the system through the corresponding adaptor. These adaptors transform the data from any other model to the internal MARISA Data Model or make it compliant with the CISE network. Thus, the design of the Data Model assures the compliance with data protection regulations, given that this model must not directly depends on any implementation of a given service. The corresponding service will not access the private messages exchanged between users and the data processed (public by definition). It is also supposed that sensitive data will be anonymized as soon as they are received and not to be stored in the system. The information entering to the MARISA Toolkit are the fused data, supposed to be privacy-by-design compliant.[6]

Evaluation

From Use Cases to Operational Trials

The MARISA project follows the Systems Engineering (SE) approach instructed by the International Council on Systems Engineering (INCOSE):[21] "Systems Engineering is an interdisciplinary approach and means to enable the realization of successful systems. It focuses on defining customer needs and required functionality early in the development cycle, documenting requirements, and then proceeding with design synthesis and system validation while considering the complete problem: operations, cost and schedule, performance, training and support, test, manufacturing, and disposal. SE considers both the business and the technical needs of all customers with the goal of providing a quality product that meets the user needs." The role of the systems engineer encompasses the entire life cycle for the system-of-interest.[30] The MARISA project life-cycle is limited to the Concept and Development Stages, as the Exploratory Research has been already performed by Consortium members and is part of their background.[30] One task of the Development Stage is to verify and validate the system, i.e. to confirm that the specified design requirements are fulfilled by the system and that the system complies with stakeholders' requirements in its intended environment. In the MARISA project, verifying and validation are carried out via operational trials one task being Data Protection Impact Assessments.

In MARISA project, the definition of the use cases has been made in previous European projects in the field of maritime surveillance (e.g. CoopP, EUCISE 2020). The selected use cases provide scenarios demonstrating how the information sharing environment is used and how to meet the user's requirements. The use cases cover all seven user communities and three processes describing the overall performance of how the information sharing system works. The three process levels are:

1) Baseline Operations: this level describes "Everyday monitoring of events in the maritime domain," or "Behaviour monitoring." The purpose of this process is to ensure the lawful, safe and secure performance of maritime activities. Furthermore, to detect anomalies (detection of possible non-compliance) and other triggers/intelligence to improve decision making for the use of response capabilities (e.g. targeting of inspections). This level also contains "simple" response to single incidents or actions within the maritime domain – everyday operations.[30]

2) Targeted Operations: the "Targeted operations" level describes operations planned in advance towards a specific activity. The purpose of this process is to react to or to confront specific threats to sectorial responsibilities as discovered in risk analysis/intelligence gathering processes. Will give support to operational decision-making when employing operational assets.[30]

3) Response Operations: Response to major incidents, events or accidents. The purpose would be to respond to events affecting many actors across sectors and borders and with a potentially major impact on, e.g. the environment and economy.[30]

The following use cases, among the whole set defined within the EUCISE2020 project, will be exercised in MARISA Project: 1) Use Case 13b: Inquiry on a specific suspicious vessel (cargo related); 2) Use Case 37: Monitoring of all events at sea in order to create conditions for decision making on interventions; 3) Use Case 44: Request any information confirming the identification, position and activity of a vessel of interest; 4) Use Case 70: Suspect Fishing vessel (small boat) is cooperating with other type of vessels; 5) Use Case 93: Detection and behaviour monitoring of illegal, unreported and unregulated (IUU) vessels listed by Regional Fishery Management Organisations (RFMOs).[30]

From use cases a continuous link with the user needs were established in order to verify the matching between the preliminary trials' objectives and the user requirements collected with the user communities. By using the systems engineering approach, the operational scenarios were defined through a certain number of parameters and the whole set of possible values which can be verified during the execution of the trials. The parameters are: 1) incident type; 2) geographic characteristics of the trial area; 3) meteo-marine conditions; and 4) the traffic conditions and target types. The selected incident types (i.e. the operational situation in which MARISA services could provide additional information) are human trafficking and smuggling; Maritime Situation Exchange and Assessment Service (MSEAS) for safety and security; irregular immigration; and safety. The geographical characteristics: i.e. the characteristics to which the trial area refers. An application domain can refer to geographical areas small or large, wide or thin, or related to the possibility to track vessels along routes. For instance, in Maritime Border Surveillance context, the interest is more focused on vessels heading orthogonally with respect to borders than on vessels sailing in parallel. The meteo-marine conditions: i.e. currents, winds, waves, temperature, etc. Meteo-marine conditions are relevant for two reasons. First of all, they can have impacts on tools performances (e.g. in the discrimination of targets with respect to the clutter). Secondarily, they define the scenarios in which MARISA services will be asked to work, and so they have to be defined in order to have a maximum added value. The traffic conditions and target types: i.e. ships densities (high / low), ship dimensions (majority of small / big ships), targets' characteristics (e.g. in terms of target motion type and speed), vessels' equipment properties (e.g. the presence of on-board ship reporting systems), vessels preferred routes (for anomalies detection), seasonal traffic variation, etc.[30]

Finally, the trails were described considering the specific goal, the area to test, the end-users and MARISA partners which will be involved, and the use cases to be tested. During the trials, a particular focus will be made on the validation of the users' assets availability, the constraints to data availability in relation to MARISA nodes installation, and the needed input data types.

At proposal stage, five operational trials for the MARISA Toolkit validation, each covering a different area and involving different partners, have been preliminary defined: 1) Northern Sea Trial (maritime situation exchange and assessment service for safety and security, end user is Dutch Coast Guard); 2) Iberian Sea Trial (irregular immigration, end users are Guardian Civil and Portuguese Navy); 3) Strait of Bonifacio Sea Trial (safety and illegal immigration, end users are PMM and Italian Navy); 4) Ionian Sea Trial (human trafficking between Corfu and Italy, end users are Greek Ministry of Defence and Italian Navy); and 5) Aegean Sea Trial (human trafficking and smuggling, end user is Greek Ministry of Defence).[30] When writing this paper, only the first trial has been carried out.

The First Trial

During the first MARISA North Sea operational trial the tested incident type was Maritime Situation Exchange and Assessment Service (MSEAS). The main goal of this trial was to validate a decision support tool in a relevant environment. The decision support tool fuses heterogeneous vessel information, detects risks and threats, and gives an advice on how to allocate the available resources for mitigation or interdiction. The decision support tool is able to extract guidelines for an open architecture that allows sustainable innovation of the surveillance and analysis systems but also for an ongoing EU-wide coastguard transformation from nautical centres to command & control centres.[30]

The Netherlands Coastguard organized a dedicated training exercise “MARISA_Alert” with three relevant operational scenarios in the maritime, security and safety domains. The MARISA_Alert exercise involved three ships of the Netherlands Coastguard: The watch ship “Guardian,” patrol ship “Visarend,” and support ship “Terschelling.” The three ships sailed ‘anomalous patterns’ as specified in the MARISA North Sea Trial scenario. The MARISA Toolkit was connected to a live feed of the Coastal Surveillance System during the demonstration of the MARISA North Sea Trial. The MARISA Toolkit was situated in the Netherlands Coastguard back-up operations facility in Den Helder. The MARISA Toolkit services successfully captured, processed, analysed and visualized in real time the maritime big data stream. The MARISA Toolkit services for anomalous behaviour detection triggered live ‘alerts’ for the Coastguard vessels sailing ‘instructed anomalous patterns' during the training exercise MARISA_Alert.[2]

Assets involved in the first trial were The Netherlands Coast Guard (NCG) Vessel Traffic Service (VTS) and AIS systems. NCG supported the definition of the capability requirement for the Maritime Situation Exchange and Assessment Service (MSEAS) for safety and security at the North Sea, provided data from its own Coastal Surveillance System (Radar, AIS) to be used in the MARISA MSEAS development, and participated in the information architecture definition required to support the development of the MSEAS. NCG analysed also data base of historic incidents to infer model information to support anomaly detection. NCG supports and hosts MARISA MSEAS data base and exchange server during the whole MARISA project for development, test & evaluation and the final demonstration.[30]

Four functional blocks were found for the MSEAS (Maritime Situation Exchange and Assessment Service): 1) data preparation and object assessment, 2) situation assessment function based on behaviour analysis and anomaly detection, 3) impact and threat assessment function to support mission planning, and 4) Secure data base and exchange system. Data preparation and object assessment complemented track coverage with additional sensor inputs and fusion. The existing Netherlands Coastguard sensor network on the North Sea was complemented with additional national sensor data from VTS chains of major ports. The track coverage from neighbouring Nations was requested for completion of the North Sea picture on the shared borders. For the tracks with known identity the heterogeneous data sources were analysed/mined to enrich the information position for the specific vessel. Extract behavioural primitives complemented the information position of a vessel. Situation assessment function based on behaviour analysis and anomaly detection included fusion of information from different sources and moments in time to enrich single vessel situation assessment reports, detection of vessels not emitting AIS messages and why (e.g. non-regulatory or illegal activities); detection of anomalous behaviour of vessels based on the complete information position, the historic database and the geographical context. Complex spatial temporal analytics was applied. Impact and threat assessment function to support mission planning detected anomalous vessels impact, threat assessment was made and reported. It also mapped threats and weighing of the potential impact and supported mission planning. The 'risk'-maps enabled the tasking of the different surveillance, safety and enforcement units. Secure data base and exchange system (PostgreSQL object-relational database with PostGIS spatial database extension) enabled multi-level access to the data.[30]

DPIA of First Trial

The first DPIA was carried out by the help of CNIL's PIA software.[22]

The MARISA Toolkit collects data from, for example, Over-the-horizon (OTH) and Photonics-Enhanced Multiple Input Multiple Output (PE-MIMO) radars, legacy systems, Automatic Identification System (AIS) and other available data sets. The first DPIA concerns on the MARISA solution/toolkit to be created and piloted during the project, and more in detail the version of MARISA during the first operational trial. During the first operational pilot, the personal data in which persons can be identified directly or indirectly included AIS data on vessels (> indirect identification), data base of historic incidents (> indirect identification) and personal data on MARISA end-users (> direct identification). AIS is a maritime technical standard developed by the International Maritime Organization (IMO). It is a radio technology combining GPS, VHF and data processing technologies to enable the exchange of relevant information in a strictly defined format between different entities. The processor of MARISA personal data is the MARISA consortium jointly, based on the MARISA Grant Agreement and Data Sharing Agreement.

In addition to the MARISA solution and its development and piloting, personal data is processed as part of the following activities: 1) MARISA websites collecting contact information for dissemination, 2) Contact information and pictures from research participants. These are however excluded in the DPIA because their privacy and data protection procedures are described in a separate privacy and data protection policy.

Conclusions

Privacy by Design (PbD) and a Data Protection Impact Assessment (DPIA) as concepts are well-known and recently many research papers have been published on this area. However, it turns out that there is not much standardization in how to actually apply PbD throughout the whole engineering process. On the other hand, new software tools are released to make the data protection impact assessment

Table 1. Design Science Research Checklist questions and answers.

Questions and Answers	This study
What is the research question (design requirements)?	section 1
How PbD and DPIA are adapted in the MAISA project?	
How to build new meta-artefacts and useful methods for the design and validation of privacy requirements engineering approaches into maritime surveillance ICT systems?	section 1
What is the artefact? How is the artefact represented?	
Guidelines for two-tiered privacy engineering: the development of the MARISA Toolkit by the research consortium and, (possible) end-use of this toolkit by relevant authorities	section 4.1
Overall Privacy-by-design framework in the MARISA Toolkit developing	section 4.2
Description of most sensitive MARISA services with regard to privacy protection	section 4.3
What design processes (search heuristics) will be used to build the artefact?	
Systems Engineering	section 5.1
How are the artefact and the design processes grounded by the knowledge base? What, if any, theories support the artefact design and the design process?	
The application domain: privacy in surveillance	section 3.1
Privacy engineering in general: PbD approach, DPIA	sections 3.2 & 3.3
The usage of social media in surveillance and how to apply PbD approach in OSINT	sections 3.4 & 3.5
What evaluations are performed during the internal design cycles? What design improvements are identified during each design cycle?	
Evaluations during operational trials	section 5
How is the artefact introduced into the application environment and how is it field tested? What metrics are used to demonstrate artefact utility and improvement over previous artefacts?	
DPIA during the first trial	section 5.3
What new knowledge is added to the knowledge base and in what form (e.g., peer-reviewed literature, meta-artefacts, new theory, new method)?	

more practical and to foster collaboration between stakeholders, and in this study we have applied a free software developed by CNIL.

Ethical issues concerning OSINT are diverse and evolving. Their impact on MARISA concern both technology, user processes and the business/governance model. Even though international regulatory guidelines are available, specific allowances, prohibitions and exceptions mainly stem from national legislation. European Data Protection Reform partly harmonizes data protection regulation in EU member states, but still leaves the possibility for variation on the national level. Big challenge in OSINT is coping with the mosaic effect. Data protection sets strong requirements on MARISA technology utilizing various data sources and performing data fusions on various levels. Another challenge concerns the reliance of automated analysis: How can data fusion algorithms that are reliable and transparent for the end-user be developed? As dos Passos argues,[23] associated with OSINT, big data is about being able to map behaviour and tendencies. However, data science is needed in OSINT because of the lack/low quality of big data, to find the correct answers, capture the correct data and to have the correct perception of how to proceed throughout the process. Current academic and public debates entertain the notion of shifting the emphasis from data collection to data analytics and data use. There are scholars who underline the need for "algorithmic accountability."[24] It can therefore be expected that the legal requirements concerning OSINT and big data may develop in this direction. Therefore, to separate the ethics of data collection from the ethics of the processing and use of data is essential.

Hevner and Chatterjee provide a general framework to guide researchers on how to conduct, evaluate, and present design science research.[1] This paper relates to these guidelines, and Table 1 answers to their design science research checklist questions. This paper presents how PbD and DPIA are adapted in the MAISA project and is a first step towards new meta-artefacts and useful methods for the design and validation of privacy requirements engineering approaches into maritime surveillance ICT systems. However, future research is needed. In the MARISA project, verifying and validation are carried out via operational trials one task being DPIA. Five trials have been defined, each covering a different area and involving different partners. When writing this paper, only the first trial has been carried out. During the rest trials more DPIAs will be carried out and their findings will be analysed and published.

References

[1] Alan Hevner and Samir Chatterjee, *Design research in information systems: theory and practice*, (New York: Springer Science and Business Media, 2010).

[2] MARISA, "MARISA Maritime Integrated Surveillance Awareness," 2018, available at https://www.marisaproject.eu/.

[3] Salvatore T. March and Gerald F. Smith, "Design and natural science research on information technology," *Decision Support Systems* 15, no 4 (1995): 251-266.

[4] EUCISE2020, "European Test bed for the maritime Common Information Sharing Environment in the 2020 perspective," 2019, available: http://www.eucise2020.eu/.

[5] MARISA, "D3.2 MARISA Services Description Document," 2018.

[6] MARISA project, "D2.6 Legal, Ethical and Societal Aspects," 2017.

[7] Erik Krempel and Jürgen Beyerer, "TAM-VS: A Technology Acceptance Model for Video Surveillance," in *Privacy Technologies and Policy, Lecture Notes in Computer Science*, vol 8450 (Cham: Springer, 2014), 86-100.

[8] Jyri Rajamäki, Sari Sarlio-Siintola, and Jussi Simola, "Ethics of Open Source Intelligence Applied by Maritime Law Enforcement Authorities," *Proceedings of the 17th European Conference on Cyber Warfare and Security ECCWS*, Oslo, Norway, 28-29 June 2018.

[9] Peter Hustinx, "Privacy by Design: Delivering the Promises," *Identity in the Information Society* 3, no 2 (2010): 253-255.

[10] Ann Cavoukian, "Privacy by Design: The 7 Foundational Principles," Information and Privacy Commissioner of Ontario (Ontario, 2011).

[11] Article 29 Data Protection Working Party, "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679," 2017.

[12] Joshua Coles, Shamal Faily, and Duncan Ki-Aries, "Tool-Supporting Data Protection Impact Assessments with CAIRIS," 2018 IEEE 5th International Workshop on Evolving Security & Privacy Requirements Engineering (ESPRE) (2018): 21-27.

[13] Michael Glassman and Min Ju Kang, "Intelligence in the internet age: the emergence and evolution of OSINT," *Computers in Human Behavior* 28, no. 2 (2012): 673-682.

[14] Douglas Wells and Helen Gibson, "OSINT from a UK perspective: Considerations from the law enforcement and military domains," in Proceedings Estonian Academy of Security Sciences, 16: *From Research to Security Union* (Tallinn, Sisekaitseakadeemia, 2017), 83-114.

[15] Bert-Jaap Koops, Jaap-Henk Hoepman, and Ronald Leenes, "Open-Source Intelligence and Privacy by Design," *Computer Law & Security Review* 29 (2013): 676-688.

[16] Bert-Jaap Koops, "Police investigations in Internet Open Sources: Procedural Law Issues," *Computer Law & Security Review* 29 (2013): 676-688.

[17] Evanna Hu, "Responsible Data Concerns with Open Source Intelligence," November 14, 2016, available at https://responsibledata.io/2016/11/14/responsible-data-open-source-intelligence/.

[18] Gašper Hribar, Iztok Podbregar, and Teodora Ivanuša, "OSINT: A 'Grey Zone'?" *International Journal of Intelligence and CounterIntelligence* 27 (2014): 529–549.

[19] C.M.K.C. Cuijpers, "Legal Aspects of Open Source Intelligence – Results of the VIRTUOSO Project," *Computer Law & Security Review* 29, no. 6 (2013): 642-653.

[20] Kedi Chen, Fengcai Qiao, and Hui Wang, "Correlation Analysis Using Global Dataset of Events, Location and Tone," *2016 IEEE First International Conference on Data Science in Cyberspace (DSC)*, Changsha, China, 2016, pp. 648-652.

[21] *INCOSE Systems Engineering Handbook*, 2019, https://www.incose.org/products-and-publications/se-handbook.

[22] Commission Nationale de l'Informatique et des Libertés, "May 2018 updates for the PIA tool," 2018, Available: https://www.cnil.fr/en/may-2018-updates-pia-tool.

[23] Danielle Sandler dos Passos, "Big Data, Data Science and Their Contributions to the Development of the Use of Open Source Intelligence," *Systems & Management* 11 (2016): 392-396.

About the Author

Jyri Rajamäki is Principal Lecturer in Information Technology at Laurea University of Applied Sciences and Adjunct Professor of Critical Infrastructure Protection and Cyber Security at the University of Jyväskylä, Finland. He holds D.Sc. degrees in electrical and communications engineering from Helsinki University of Technology and a PhD in mathematical information technology from University of Jyväskylä.