VALCRI
VISUAL ANALYTICS FOR SENSE-MAKING IN CRIMINAL INTELLIGENCE ANALYSIS

***VALCRI* WHITE PAPER SERIES**
VALCRI-WP-2017-005
1 January 2017
Edited by B.L. William Wong

The Operationalisation of Transparency in VALCRI

Eva Schlehahn[1], Penny Duquenoy[2], Pragya Paudya[2]l, Carlisle George[2], Fanny Coudert[3], Audry Delvaux[3], and Thomas Marquenie[3]

[1]Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Kiel, Germany
[2]Middlesex University, London, UK
[3]KU Leuven Centre for IT & IP Law, Leuven, Belgium

Project Coordinator
Middlesex University London
The Burroughs, Hendon
London NW4 4BT
United Kingdom.

Professor B.L. William Wong
Head, Interaction Design Centre
Faculty of Science and Technology
Email: w.wong@mdx.ac.uk

EUROPEAN COMMISSION

INTENTIONALLY BLANK

ABSTRACT

This White Paper presents some research and findings from the EU-funded R&D project VALCRI with regard to the requirement of transparency from legal, ethical, and data protection perspective. Thereby, it addresses difficulties of transparency operationalization and presents possible solution approaches, which are linked to recent R&D in the realm of data, process and reasoning provenance.

Keywords

Crime Analytics, Transparency, Legal, Data Protection Law, Ethics, Provenance.

INTENTIONALLY BLANK

INTRODUCTION AND SCOPE OF THIS PAPER

Nowadays, law enforcement agencies (LEAs) increasingly integrate Big Data analytics tools in their daily work to support the fulfilment of their investigative and preventive tasks. Typical for these systems is the connection of persons and assets to find patterns and correlations related to crime, such as the determination of crime hot-spots, or the detection of organised and serial crimes. Statistical information about past crimes is used to ascertain incidents and to decide upon actions like some operational, tactical, or strategic activities of the responsible police forces.

In this context the VALCRI project (Visual Analytics for Sense-making in Criminal Intelligence Analysis) is focused on building a criminal intelligence analysis prototype which provides tools to extract and convert unstructured data from mixed-format sources, aggregate it (e.g. for crime statistics and individual case analysis) or to find organised and serial crime via similarity analysis, filtering and clustering of data. Thereby, VALCRI aims at visualizing the analysis results in various structures and forms, e.g. sorted by crime types, location, or by time frame to support the work of police analysts.

Analytic tools of this kind are often promised to deliver an accurate risk assessment, enabling law enforcement not only to investigate past crimes better, but eventually, also to anticipate events before they actually happen. On the LEA side, therein lies the hope to acquire the necessary knowledge to address roots of crimes as well as to react in a timely fashion to prevent criminal activities. But crime analytics is also often criticised as being dangerous for fundamental rights and civil liberties of citizens. Advocates of citizen rights and the media frequently admonish the inherent risks of misuse and bias, usually coming along with a severe lack of transparency.

In this context, it is important to realise that Big Data-supported analytics of crime are so powerful nowadays that the further step towards more prediction-focused criminal intelligence tools appears not very far. On the basis of software generating just statistics-founded information about past crimes to support criminal investigation, the further broadening of the software capability in order to even predict future events is in fact quite easy, though out of the scope of this current project.

Regardless of the actual context, transparency has long been known as one of the most essential factors to enable the trust of citizens in their government [Welch, Hinnant, 2003]. Furthermore, challenging decisions based on analytics results is very difficult when the used criteria and parameters are not known at all. In the long term, such a situation leaves an imprint of fear on any freedom rights exercise, which affects not only the individual citizen, but also the society as a whole. So it comes as no surprise that such insecurity issues also severely impinge upon the public view of police integrity and misconduct [Rosenbaum, 2016].

Cognitive bias also plays a role, with a heated public debate about algorithms using parameters related to the societal or socioeconomic status, or the race of persons instead of being limited to mere spatio-temporal data sets to perform their estimates [Angwin, Larson, Mattu, Kirchner, 2016]. A number of different cognitive bias types have been proven to be very relevant for the specific context of criminal intelligence analysis. These are for example confirmation bias, anchoring and adjustment effect, clustering illusion, framing effect, availability heuristics, base rate fallacy, selective perception, and group think. Thus, it becomes clear that the mitigation of biases is a significant topic in ongoing cognitive psychology research [Hillemann, Nussbaumer, Albert, 2015]. Moreover, the classical 'Garbage in, garbage out' principle applies to any LEA Big Data analysis, whereas serious repercussions can occur for the individual citizen concerned. Potential shortcomings regarding the accuracy of algorithmic results could occur when the existence of unrecorded cases must be taken into account. Therefore, the current lack of meaningful evaluation raises scepticism about the effectiveness of crime analytics systems [Borchers, 2016].

So consequently, transparency appears necessary for a number of reasons in crime analytics. Thereby, it is important not only for the concerned individuals, but also for the police and supervisory authorities for evaluation and monitoring purposes [Danezis et al., 2014, chapter 2.2 p. 9].

OVERVIEW OF APPLICABLE LEGAL FRAMEWORK

In Europe's democratic societies, human rights are quintessential elements to establish and safeguard the balance between the liberty and security of citizens. Crime analytics can be a useful tool for LEAs, yet comes along with inherent risks for fundamental rights of individuals. With every small bit of information potentially becoming relevant in a crime context, governmental institutions covet the increasing collection of personal data, thereby ignoring the dangers of unintentional or even intentional misuse. Especially at stake are core principles like the presumption of innocence, the right to due process and fair trial, and non-discrimination.

With regard to transparency, the Rule of Law must be seen as most relevant since it is a core pillar of democratic societies. It sustains necessary limitation of governmental power to protect the fundamental rights of citizens. However, the Rule of Law extends not only over governmental institutions, but has an all-encompassing nature, binding persons, as well as public and private entities alike [Secretary General of the United Nations, 2004]. In Europe, the Rule of Law - besides Human Rights and democracy - is increasingly interpreted in a broad and holistic manner to respect human dignity. Furthermore, this serves to provide

meaningful concepts as guidance for their operationalisation. However, its realisation continues to be a difficult and on-going process both on the European as well as on the national level [Timmer, Majtényi, Häusler, Salát, 2014]. Thereby, a degree of transparency about the goals of governmental actions, the necessity and proportionality of measures, and the means of their execution is required [cf. Austin, 2015].

European Data Protection Law requiring transparency

The protection of personal data is a fundamental right, first acknowledged by the European Convention of Human Rights and then further manifested in the European data protection framework and the corresponding national laws of the EU member countries. The reform of the European data protection reform, coming into full effect by May 2018, has an impact on modern forms of Big Data analytics as well. The protection of personal data gains more momentum by a set of amended rules in the new General Data Protection Regulation (GDPR). These rules encompass not only the processing cycle of information, but also require better transparency regarding algorithmic decision-making [Chiel, 2016]. For the police and justice sectors, the European data protection reform resulted in the Directive (EU) 2016/680, which regulates the processing of personal data in these areas. But in comparison to the GDPR, the directive has put some limits on the requirement of transparency by restricting the right of the data subject to be informed and to gain access, and on the obligation of the LEAs to notify the data protection supervisory authorities about their data processing activities. Naturally, a suspect of a crime will never have direct access to a crime analytics system of a law enforcement agency. Also, during an ongoing investigation, LEAs might have the right to deny full disclosure of their actions or the case files on the basis of the respective country's criminal laws to ensure the perpetuation of evidence. So while being focused on the protection of personal data of individuals, the new Directive (EU) 2016/680 still has mechanisms in place to support the effectiveness of police and justice work.

However, this does not mean that in the police and justice sectors, no transparency is required at all. Rather, Article 15 of Directive (EU) 2016/680 foresees that the EU member countries regulate these limitations in their national law, providing for clear and explicit exemption cases restricted to the application cases the directive mentions. Furthermore, the factual or legal reasons for the denial of data subject's rights must be documented, while this documentation must be made available to the competent supervisory authorities. Also, according to Article 17, such supervisory authorities may help the data subject in exercising the rights guaranteed by the law and thus can serve as intermediaries between individuals and the LEAs. Corresponding to this, Article 26 of Directive (EU) 2016/680 directly requires the cooperation with the supervisory authority on request.

Moreover, the allowance of specific cases with limitations to the right of access is compensated by other, specific transparency obligations, which must be supported by corresponding organisational and technical measures. For example, the Articles 24 and 25 require the records and the logging of processing activities. Or, as another example to demonstrate the general demand for transparency, the controller of a processing activity must be able to demonstrate compliance with the data protection law according to Article 4 (4) of Directive (EU) 2016/680. This may also serve compliance statements related to criminal procedure provisions. So this specific article manifests a specific interest of the controllers themselves to respond to eventual accountability issues. Thereby, it is useful to note that the interests and involvement of different stakeholders (besides the data subject) are covered by the explicitly stated purposes for which logging functionalities should be implemented. Pursuant to Article 25, subsection 2, logs shall be used solely for the verification of the processing lawfulness or self-monitoring, or to ensure the integrity as well as the security of the personal information, and for criminal proceedings. So overall, it can be said that transparency is important for a number of various entities. Of course, the main focus in the Directive (EU) 2016/680 lies on the data subject, who is in need of protection. Likewise, competent supervisory authorities need information about the processing activities to exercise their oversight work. Likewise, the LEAs need transparency for accountability reasons, which means the demonstration of compliance not only with data protection law, but also to serve their own disclosure obligations in criminal trials. Ultimately, to achieve adequate transparency, its scope needs to be quite wide. This is backed up by EU legislators as well since Recital (38) of Directive (EU) 2016/680 clarifies that:

'*The data subject should have the right not to be subject to a decision evaluating personal aspects relating to him or her which is based solely on automated processing and which produces adverse legal effects concerning, or significantly affects, him or her. In any case, such processing should be subject to suitable safeguards, including the provision of specific information to the data subject and the right to obtain human intervention, in particular to express his or her point of view, to obtain an explanation of the decision reached after such assessment or to challenge the decision.*'

So with the reform of the data protection framework, the legislators have widened the understanding of transparency. Before, the law has only known the processing cycle of the information itself as the solely relevant focus [cf. Hansen, Jensen, Rost, 2015], yet now the decisions based on said personal information must be taken into account as well.

As a result, transparency needs to be defined as the property that **all data processing** – meaning all operations on data including the legal, technical, and organisational setting – **and the correlating decisions** based on the results

can be understood and reconstructed at any time. With regard to not only data protection law, but also criminal procedure laws, this requires **openness, legal clarity** and **certainty** in relation to all aspects of the criminal intelligence analysis process.

Widening the scope of transparency in such a way makes it possible to develop a concept of transparency which recognises its value as a mandatory principle to be followed. Of course, nature, scope and extent of transparency are always dependent on the context, the circumstances, and the involved actors. This makes it difficult to accommodate to the individual cases in question and to determine concrete measures required. Also, transparency is often seen differently in its level of obligation, whereas some see it merely as 'meta-legal' principle or 'ancillary obligation' in relation to the underlying applicable legal norms. Yet, transparency always has some kind of normative value, making it relevant as an essential element in democratic governance. Thereby, it is equally technique (e. g. for accountability) as well as a norm (e.g. for legitimacy) while the distinction of mere information and knowledge definitely matters [Hernández, 2014]. On this account, the above definition demands a comprehensive understanding of data processing and the related decisions – a scope covering all relevant aspects needed to support an adequate level of protection for citizens whose personal information is being processed.

Criminal procedure and transparency - Disclosure

Transparency is widely considered a key precondition for the safeguarding of human rights in the criminal investigation process. For a suspect to fully exercise his or her right to a fair trial, a comprehensible and clear procedure must exist to inform the involved parties of their role and rights, and to allow understanding of the reasoning behind the charges brought against them. While it is generally accepted that the unique nature of criminal procedure does not always allow immediate and full insight into all police and judicial activities, it is considered necessary for a fair trial that accused and their defence teams are given access to some collected evidence and, under circumstances, additional police information.

The UK has an adversarial system, regarding the conduct of criminal trial/proceedings (similar to many common law countries). The prosecution presents arguments and evidence in a court of law before a third party (e.g. judge and jury) with the objective of demonstrating 'beyond reasonable doubt' that an accused (defendant) is guilty of a crime. The accused is represented by his defence team whose duty is to present arguments and evidence to the court to challenge and raise doubt regarding the prosecution's case. The process of a criminal trial is governed by various rules and procedures, many of which safeguard the rights of an accused. Among many of these rules is the 'golden rule' of disclosure to ensure fairness [Plater and de Vreeze, 2012], i.e. each side (prosecution and defence) must disclose certain relevant materials to each other. Disclosure is a fundamental element of an individual's right to a fair trial under Article 6 of the European Convention on Human Rights. In the UK, the process of disclosure is mainly governed by the Criminal Procedure and Investigations Act 1996 (CPIA) and the CPIA Code of Practice. Under the Act (Section 3), the prosecutor must disclose all material held by the prosecution team that is capable of undermining the case against the accused or assisting the case for the accused. Some material obtained in a criminal investigation (e.g. sensitive material protected under a Public Interest Immunity Certificate) is exempt from disclosure obligations. The duty of disclosure starts pre-trial, and extends to all stages of criminal proceedings, i.e. there is a continuing disclosure obligation on the prosecution throughout a criminal trial (Section 7A, CPIA). Failure to meet its disclosure obligations may result in various sanctions against the prosecution, such as, a judge may stay proceedings against an accused (i.e. the case is struck off), prosecution evidence may not be admitted in court or costs can be awarded against the prosecution [Cross and Treacy, 2012].

The CPIA (Section 23(1)) Code of Practice provides important definitions and details the various roles and responsibilities of police officers involved in a criminal investigation (including 'investigator' and 'disclosure officer'). The investigator has a duty to retain material obtained during a criminal investigation that may be relevant to the investigation. The disclosure officer is responsible for examining material collected during an investigation, revealing such material to the prosecutor and also disclosing material to the accused if requested to do so by the prosecutor. Section 2.1 of the Code states that 'material' can be "*of any kind, including information and objects, which is obtained or inspected in the course of a criminal investigation and which may be relevant to the investigation. This includes not only material coming into the possession of the investigator (such as documents seized in the course of searching premises) but also material generated by him (such as interview records)"*. Further "*material may be relevant to an investigation if it appears to an investigator, or to the officer in charge of an investigation, or to the disclosure officer, that it has some bearing on any offence under investigation or any person being investigated, or on the surrounding circumstances of the case, unless it is incapable of having any impact on the case*";

The Disclosure Manual of the Crown Prosecution Service (CPS, 2016) addresses the issue of information recorded on a computer at Chapter 5, Sections 5.21. – 5.23. Section 5.22 mandates that prosecutors need to be informed of the use of such computer systems and need to be able to inspect material held on these systems. It also states that the defence may be given supervised access to the terminal screens of such systems or where acceptable the information may be supplied to them on a disk.

Arguably, the use of VALCRI for analysis can result in the production of material relevant to an investigation, (e.g. to support the theory of a crime) and presented during the

course of a criminal trial as documentary exhibits. For example analysis chats, maps, similarity lists and associated records can be used to make connections during an investigation to establish probable cause leading to suspicion and possible arrest. A practical example is that a person P1 is arrested and based on analysis using VALCRI, data from P1's phone is linked to a known criminal gang. The frequency and duration of calls, as well as geo-location data demonstrated in charts produced by VALCRI (showing linkages between various people) may lead an investigator to establish suspicion and probable cause for further arrests. Equally use of VALCRI may result in the production of material (from analyses) that would potentially undermine a prosecutor's case or assist the defence. Both types of material are relevant and potentially disclosable. Transparency in VALCRI therefore includes managing the provenance of material relevant to each criminal investigation in light of disclosure obligations under UK criminal procedure.

As opposed to the adversarial approach taken in the United Kingdom, Belgium adheres to the tradition of civil law and employs an inquisitorial procedure in its penal system. An essential difference between the adversarial and inquisitorial systems is the issue of 'disclosure', between opposing parties. While certain details and practical matters may differ, the Belgian system described below is largely representative of other inquisitorial systems in Europe. In such a system, the courts are heavily involved in the investigatory phase of criminal proceedings and are tasked with collecting and reviewing both incriminating and exculpatory evidence. The prosecutor has a combined role of convicting criminals and making sure that the trial is fair. The defence has little power to conduct investigations [Ringalda, 2010]. This contrasts with the adversarial system where the prosecution/state is mistrusted and both the prosecution and defence have the power and right to carry out their own investigations and present their own case [Ringalda, 2010].

The Belgian legal system distinguishes between two stages in the criminal procedure. During the non-contradictory pre-trial investigative phase, access to the criminal file and collected evidence is limited to persons with a direct interest filing a request with the public prosecutor or investigating judge (Article 21bis of the Belgian Criminal Code of Procedure). At the end of the investigatory stage, records of all evidence collected during the investigatory stage should be made available to the judge, prosecution and defendant ahead of the actual trial in court, which takes place in a public manner and involves open discourse between the parties (Article 127§2 of the Criminal Code of Procedure).

The information which is disclosed to the defendant is generally and strictly limited to evidence, which consists of certain reports, findings and outcomes of investigations included in the criminal file. This means that only the final report produced by the criminal analyst will be attached by the prosecutor to the criminal file and then disclosed to the parties involved. The so-called 'start' information or provenance of police intelligence, being information used only to trigger an investigation or steer it in a certain direction (i.e. some of the information produced by the VALCRI system), will have to be notified to the trial court or the parties involved if it is part of the evidence, which is rarely the case. The general rule is thus that intelligence is not disclosed.

However, in two recent cases, the Belgian Court of Cassation (10 September 2013 P.13.0376.N/1 and 25 November 2014 P.14.0948.N/1) ruled that intelligence had to be disclosed whenever the defence made plausible and credible beyond mere assertion that the intelligence was obtained illegally. The defence does not have to demonstrate that the provenance is unlawful, but have to provide sufficient elements that point towards a potential infringement by police of the rules applying to intelligence gathering. A mere assertion by the defence in that sense is not sufficient as there cannot be a presumption of unlawful collection of evidence. The Judge decides supremely about the elements brought by the defence. As a way of example, in the most recent case, the police had received information about a potential illegal culture of drugs and decided to open an investigation. The defence was claiming that the police used proactive methods of investigation to obtain this information without the mandatory prior legal authorisation. The judge asked the Prosecutor, who is subject to a duty of loyalty and integrity, to clarify whether the claim had sufficient ground. The Prosecutor considered that this was not the case. Without any additional elements of suspicion brought by the defence, the Judge rejected the claim.

VALCRI only processes information whose source is presumed lawful and does not alter in any way the source of the information. Claims of the defence about the illegality of the way how the information has been collected could not be solved by accessing the information stored in VALCRI. However, if the defence would challenge the further use of this information by the police, the Prosecutor or the Inquiry judge could ask them to demonstrate that the claim is unfounded. Ensuring the full traceability of the use of the information throughout the system thus becomes paramount. VALCRI's functionalities on data provenance, traceability and recordkeeping will assist in resolving these issues and any concerns about the legality of the use of the information once entered into the system.

ETHICAL CONSIDERATIONS

From an ethical perspective, transparency is important because of its role in making actions and processes visible. This visibility provides an opportunity to understand, verify, or question, the logic and validity behind the stages of dec sion-making. In the context of law enforcement and the pursuit of justice, this is crucial[1] both in terms of demon-

[1] See for example Open Government Programme (OGP), under Law Enforcement: Increasing Public Integrity, the first in the list of activities is:

strable processes and validity of reasoning and evidence (for the courts/justice system). Transparency in actions and decision-making is one of the principles of the College of Policing Code of Ethics [2014, p.3] under the heading of 'Openness'. Those working in policing are required to be '*open and transparent in […] actions and decisions'*.

The VALCRI system is designed to aid the police in making decisions. And in mediating the processes undertaken by police in their duties, the VALCRI system should be designed to reflect the ethical principles espoused by their professional body. Accountability is also a principle in the College of Policing Code of Ethics (ibid), therefore when technology is used to help intelligence analysts, the technology[2] also needs to be accountable – that is, to be able to show the actions taken by the system, literally acting as a 'aide'[3] on behalf of the Intelligence Analyst. To achieve this, transparency is also required of the processes and operations 'of' the system and 'on' the system, which need to be made visible in an appropriate way, for example logging user actions and system changes.

One of the difficulties in achieving total transparency of the system actions in the design and development of VALCRI is that different algorithms have been used which, given the opaque nature of the algorithms, raises concerns related to algorithmic decision-making. The lack of transparency in this particular process makes it harder to understand the rationale behind any particular decision. And this raises important questions relevant to openness and accountability, as well as other principles in the College of Policing Code of Ethics such as fairness and integrity (i.e. integrity of the information provided to the analyst). On the other hand, transparency in the VALCRI system aids the law enforcement agency's analytical work concerning the identification of (i) the datasets that have been used, (ii) the features/variable/ attributes that were used in the analysis, and (iii) the weighting of the features. These aspects can be used in some part to rationalise decisions made. It has also been said [Datta et. al.; 2016] that by making the processes clearer, this enables the analyst to more easily identify bias, and correct errors – addressing the principle of fairness in reducing the risk of discrimination (e.g. ethnicity, gender).

Including ethics in the system design means translating principles that support ethical behaviour (and constrain unethical behaviour) in the requirements process either directly (using the example of logging, above), or by looking at the range of requirements to how ethical considerations may be relevant. Establishing transparency of operations (system and personnel) is in response to the claim that computers have certain characteristics that can create ethical issues [Moor, 1985]. One of those characteristics is the "invisibility factor" which applies in three ways:

(i) invisible abuse (i.e. to take advantage of the invisibility factor to act unethically, e.g. to adapt the program to remove or alter confidential information);

(ii) invisible programming values, which may not be consciously recognised but which influence decisions made by the programmer (e.g. to interpret ambiguous requirements, or make other judgments) that become embedded in the product, and which are not necessarily visible to people running the program, and

(iii) invisible complex calculations, which are beyond 'human comprehension'.

These are pertinent to the VALCRI system, and some are easier to address than others. For example, item (i) is addressed by tracking changes in the system and any changes in the information accessed by end user retrieved from the system through logging mechanisms, as well as security measures. Programming values (ii above) are partially addressed by feedback processes between the developers and the end-users, and can also be addressed in training material if necessary (through explanations of how the system behaves in the case of a search, for example). Invisible complex calculations, such as the use of algorithms, are more challenging in terms of 'visibility' – it is not yet clear how to make these operations transparent. However, VALCRI is a decision-support system, offering results to the Intelligence Analyst who would use their skills to recognise what is significant and relevant.

Ethically, information provided whereby the selection reasoning and trail cannot be demonstrated (as in the case of algorithms) cannot be the determining factor, or grounds, for identifying a suspect. This is supported, as noted in the legal perspective section, in the statement referring to the right of the person (data subject) '*not to be subject to a decision … based solely on automated processing […]*'. It is important that developers and end-users recognise the limitations of what technology can provide in different contexts [EGE, 2014]. What may be useful in one context may not be appropriate in another (for example, profiling for marketing and profiling to identify potential criminals have very different implications for a person).

TYPICAL APPROACHES OF TRANSPARENCY REALISATION

Transparency in crime analytics must be realised based on the context of actual deployment [Danezis et al., 2014, ch. 4.11 p. 44 ff.]. Therefore, the scope of implementation must encompass not only the technology itself, but also the comprehensive organisational and regulatory circumstanc-

Promoting transparency, accountability and public participation on police and public prosecution service.
http://www.opengovpartnership.org/tags/law-enforcement

[2] Also recognised by OGP is the use of technology 'We commit to supporting and developing the use of technological innovations by government employees and citizens alike. *We also understand that technology is a complement, not a substitute, for clear, useable, and useful information.'* [italics added]
http://www.opengovpartnership.org/about/open-government-declaration

[3] As an assistant, helper, advisor.

es under which this IT system will be used [Gürses, Troncoso, Diaz, 2011]. Several aspects play a role in this context, for example the need to provide transparency for:

- re-tracing and understanding past events
- showing the technical and organisational setup
- avoiding or mitigating possible future issues

To approach these goals comprehensively, it is always necessary to evaluate the intended context of deployment. This is to determine which measures are suitable to provide meaningful evidence for compliance with legal and ethical requirements. Typical example measures for the realisation of transparency with regard to the above mentioned aspects are:

- Verification of data sources
- Documentation of IT processes
- Documentation of institutional procedures
- Documentation of testing
- Documentation of (related) contracts
- Logging of accesses & changes of the data
- Versioning of different prototypes/systems
- Keeping track of data, especially evidential material and other data essential for decision-making during an investigation
- If consent to the processing of personal information plays a role in the deployment context: documentation of consent and its status, e.g.: given/refused/withdrawn

With regard to the technological solutions, different advances are being made in the current R&D landscape. Generally, all of them aim at more efficiency regarding the implementation of transparency, whereas various approaches are being taken. For example, a number of researchers focus on the interpretability of the data processed, recognising the issue of knowledge extraction from data regularity patterns as the paramount requirement for the successful distribution of analytics software in real-world applications.

Several research outlets found that supporting objective interpretability of processed data may help to detect, reinforce and mitigate prejudice and cognitive biases. Thereby, they mostly focus on different ways to achieve information reduction, ranging e.g. from mere graphical tools and dimensionality reduction to more advanced class similarity/dissimilarity measuring. However, this field of research is currently very in flux, and solutions are still heavily context dependent [Vellido, Martín-Guerrero, Lisboa, 2012]. Another example is research focusing on formalizing transparency reports through Quantitative Input Influence (QII) measures capturing the degree of influence of the data input on algorithmic output and decisions [Datta, Sen, Zick, 2016].

However, it remains to be seen how well the adoption of these various research progresses, especially with regard to the rather high ex-post transparency obligations in the LEAs sector.

RESULTING DESIGN REQUIREMENTS FOR VALCRI

The VALCRI project aims at providing a system prototype which supports the semantic extraction of data from multiple and mixed-format sources. Thereby, the question is how appropriate transparency-enhancing measures can be implemented. Transparency means in other simpler words, the verifiability of the data usage with reasonable effort and at any time. This is supposed to help LEAs demonstrate compliance with the law and should ideally involve the complete lifecycle of the data. As made apparent above already, transparency needs to be realised on a technical as well as on an organizational level. The correlating research in VALCRI has found that the requirement of transparency has a strong connection to the provenance of IT systems. Thereby, provenance is to be understood as a set of measures and tools enhancing the insight into the processing operations of the system. This insight requires a comprehensive approach which covers three different dimensions:

- Data provenance
- Process provenance
- Reasoning provenance

Data provenance entails the information about which kind of data is being used, and its quality. Data origin or source, and the processing flow (including information about senders and recipients) are also part of it. The goal is to track and record the processing operations, which may also help in pinpointing eventual uncertainties e.g. regarding the completeness, accuracy, reliability, and relevance of the information. Process provenance aims at tracking the analytics processes themselves to enable the already above mentioned interpretability of their outputs. This requires some degree of transparency in relation to algorithmic parameters, as well as the components or tools used. Reasoning provenance focuses on the user of the analytics system in order to document the workflow and the decisions taken based on the analytics results [Beecham et al., p. 5 f. + p. 12 f., 2015]. Grounded on the aforementioned aspects, a comprehensive concept for the development and deployment of crime analytics is needed. This requires the implementation of several elements, which are:

- A comprehensive data model
- Adequate and complete system documentation
- Support of uncertainties awareness on UI side
- User documentation of the reasoning process
- Facilitation of meaningful, i.e. interpretable output
- Backend security logs on user and system activities

This list cannot be conclusive, due to the context-dependency of the circumstances of a real-world usage of crime analytics software. However, these are measures complementing each other, covering the above mentioned

three domains of provenance. In VALCRI, a number of concrete provenance ontology requirements have been developed, while some of them are strongly related to each other and some partial overlaps are existent. This is intentional to provide a rather comprehensive coverage of the different provenance domains. So the provenance requirements identified during the project runtime so far are:

- Analyst actions and decisions

The low-level actions of the analysts are captured and collected in a workflow, and ultimately grouped in a session. The individual steps of the workflow are stored and made retrievable on demand, including queries, the reasons for querying (e.g. working on a certain investigation), and the viewed query results.

- Analyst data

Much of the provenance information needs to be connected to the user, i.e. analyst. The user is represented somewhere in the system, e.g. with a user name or other identifier, so recorded provenance data must enable the linkage to the specific user logged in and triggering the system activities. This information may be combined with backend and security log information.

- Data changes

VALCRI will not change any data in a source database. But of course, changes of information in the source DB itself are possible, for example the deletion, modification/alteration, merging, and addition of data. So some kind of synchronization is needed to make sure the VALCRI information is always up to date and correct. Diverse options are still discussed, ranging from optimal solutions for updating, flagging, blocking, and deletion procedures, plus notifications of analysts in form of specific change logs within customizable time intervals. Getting into more detail regarding this requirement is still an on-going process to shape the technology ideally to the specific institutional needs of the LEA end users.

- Data context

Information about the context of the data (judicial decisions, acts not to prosecute or the like) needs to be stored and be retrieved from the source DB. This entails the rules on how to handle the data, while this requirement is strongly related to the data quality and restrictions on data requirements (see below).

- Data origin

The time, date and origin of the data must be stored and be retrieved from the source DB when it is loaded into VALCRI. This requirement affects the RDF transformation and import component of VALCRI performing the data ingestion/input of data and eventual metadata necessary to attach.

- Data quality

Information about the quality of the data needs to be stored and retrieved from the source DB. Furthermore, it must be possible to annotate data with its quality (e.g. via a "trustworthiness scale" of various sources), while the challenge here is to develop a solution which fits the different levels of granularity with which the different LEA end users work in their countries. Furthermore, the "probabilities" of the processing results need to be reflected and made visible to the user.

- Process and reasoning provenance

Enable traceability of what the system has done and based on what data, e.g. components executing certain algorithms on certain pieces of information within the system to avoid the algorithmic processes being a black box to the user. Furthermore, reasoning of the analyst must be made explainable by capturing of the whole lifecycle of the data processing operation and whole user “session”. This requirement is related to the following other provenance requirements: Saving the state of a widget, Analyst actions and decisions.

- Restrictions on data

The analyst should be able to attach information about restrictions of further processing of the data, data quality, etc. to the information/intelligence generated by VALCRI. This includes information about certain retention rules and further access preconditions.

- Retrieving and moving data

Information about when and from where data has been moved (within the system - for external moves, see related requirement stories) must be stored and be retrievable. This includes every query that is sent to the storage, with its parameters, date and time of the query.

- Saving the state of a widget

In order to track the reasoning (analytical) provenance, the system must be capable of storing and retrieving the state of a widget. This could be compared to a "bookmark" of a state that the user wanted to be able to go back to. The state can be annotated and should be saved including the data that it has.

- Sessions and purpose

For documentation reasons, some notion of a session/task with an attached user must be stored and made retrievable. This relates to the VALCRI-specific environments and canvases in the AUI. So when a user opens a new "environment"/canvas, it then is related to a task, e.g. working on a specific case, a pattern detection analysis, crime statistics, or something else in the context of the typical LEA work. Such a task eventually spans several logins. This way, the user is enabled and triggered to enter a purpose for the session, while this might probably be grouped with other provenance information that is captured during a "session", i.e. steps, queries, and decisions belonging to a certain "session".

Those requirements in sum are meant to address all of the three provenance domains comprehensively. How some of these are implemented will already be described in the parallel White Paper ‘Analytical Provenance for Crimi-

nal Intelligence Analysis' [Islam, J; Anslow, C.; Xu, K.; Wong, W., 2016], yet the detailed realization of these provenance requirements (and thus transparency) is still an on-going process of further refinement that continuously goes along with the technical development.

REFERENCES

Angwin, J.; Larson, J.; Mattu, S.; Kirchner, L. (2016). 'Machine Bias - What Algorithmic Injustice Looks Like in Real Life'. Article published at propublica.org.

Austin, L. M. (2015). 'Surveillance and the Rule of Law'. Debate article published in the Surveillance & Society Journal Vol 13, No 2 (2015).

Beecham, R.; Vogiazou, Y.; Bielska, A.; Viehmann, C.; Sacha, D.; Rooney, C.; Xu, K.; Anslow, C. (2015). 'User Interface Design for Uncertainty Representation and Analytic Provenance Representation'. Deliverable No. D.4.6 of the VALCRI project (Visual Analytics for Sense-Making in Criminal Intelligence Analyis).

Borchers, D. (2016). 'Predictive Analytics bei der Polizei: Tätergruppen als Schlechtwetterfront entlang der Autobahn' (Engl.: 'Predictive Analytics at the police: Offender groups as bad weather front along the Autobahn'). Article published at heise.de.

Chiel, E. (2016). 'EU citizens might get a 'right to explanation' about the decisions algorithms make'. Article published at fusion.net.

College of Policing, 2014. 'Code of Ethics - A Code of Practice for the Principles and Standards of Professional Behaviour for the Policing Profession of England and Wales'. Copyright College of Policing Limited, Coventry, England. Revised text accepted by the British Parliament as code of practice in July 2014.

CPS (Crown Prosecution Service). 'Disclosure Manual'. Chapter 5, available at: http://www.cps.gov.uk/legal/d_to_g/disclosure_manual/disclosure_manual_chapter_5/

Cross, L. J. and Treacy, L. J. (2012), 'Further review of disclosure in criminal proceedings: sanctions for disclosure failure'. Judiciary of England and Wales, November 2012.

Danezis, G.; Domingo-Ferrer, J.; Hansen, M.; Hoepman, J.; Le Métayer, D.; Tirtea, R.; Schiffner, S. (2014). 'Privacy and Data Protection by Design – from policy to engineering'. European Union Agency for Network and Information Security (ENISA)

Datta, A.; Sen, S.; Zick, Y. (2016). 'Algorithmic Transparency via Quantitative Input Influence: Theory and Experiments with Learning Systems'. IEEE Symposium on Security and Privacy (SP), pp. 598-617.

EGE, 2014. 'Ethics of Security and Surveillance Technologies'. Opinion No. 28 of the European Group on Ethics in Science and New Technologies, Brussels, 20 May 2014.

Gürses, S.; Troncoso, C.; Diaz, C. (2011). 'Engineering Privacy by Design'. Conference on Computers, Privacy & Data Protection (CPDP 2011).

Hansen, M.; Jensen, M.; Rost, M. (2015). 'Protection Goals for Privacy Engineering'. Proc. 1st International Workshop on Privacy Engineering, IEEE 2015.

Hernández, G. I. (2014). 'Turning Mirrors into Windows? Reflections on Transparency in International Law'. the journal of world investment & trade Vol. 15. (2014) 1087-1107.

Hillemann, E.-C; Nussbaumer, A.; Albert, D. (2015). 'The Role of Cognitive Biases in Criminal Intelligence Analysis and Approaches for their Mitigation'. European Intelligence and Security Informatics Conference (EISIC), 7-9 September 2015, Manchester, UK.

Moor, J.H. (1985). 'What is Computer Ethics?'. Metaphilosophy, 16:266-275, 1985 doi: 10.1111j.j467-0073. 1985.tb00173.x

Plater, D. and de Vreeze, L. A., (2012). "Is the 'Golden Rule' of Full Prosecution Disclosure a Modern 'Mission Impossible'?". 14 Flinders L.J. 133, 2012, November 22, 2012.

Ringnalda, A. (2010). 'Inquisitorial or Adversarial? The Role of the Scottish Prosecutor and Special Defences'. Utrecht Law Review Vol. 6 No. 1, 2010.

Rosenbaum, D. P. (2016). 'Special issue on police integrity: an introduction'. Policing: An International Journal of Police Strategies & Management, Vol. 39 Iss: 2

Secretary-General of the United Nations (2004). 'The rule of law and transitional justice in conflict and post-conflict societies'. Report published for the UN Security Council August 23rd 2004 (S/2004/616).

Timmer, A.; Majtényi, B.; Häusler, K.; Salát, O. (2014). 'Critical analysis of the EU's conceptualisation and operationalisation of the concepts of human rights, democracy and rule of law'. Deliverable No. 2 in Work Package 3 (D3.2) of the Frame project (Fostering Human Rights among European Policies).

Vellido, A.; Martín-Guerrero, J. D.; Lisboa, P. J. G. (2012). 'Making machine learning models interpretable'. ESANN 2012 proceedings, European Symposium on Artificial Neural Networks, Computational Intelligence and Machine Learning.

Welch, E. W.; Hinnant, C. C. (2003). 'Internet Use, Transparency, and Interactivity Effects on Trust in Government'. Published in the proceedings of the 36th Hawaii International Conference on System Sciences 2003.

The research leading to the results reported here has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) through Project VALCRI, European Commission Grant Agreement Number FP7-IP-608142, awarded to Middlesex University and partners.

	VALCRI Partners	**Country**
1	Middlesex University London Professor B.L. William Wong, Project Coordinator Professor Ifan Shepherd, Deputy Project Coordinator	United Kingdom
2	Space Applications Services NV Mr Rani Pinchuck	Belgium
3	Universitat Konstanz Professor Daniel Keim	Germany
4	Linkopings Universitet Professor Henrik Eriksson	Sweden
5	City University of London Professor Jason Dykes	United Kingdom
6	Katholieke Universiteit Leuven Professor Frank Verbruggen	Belgium
7	A E Solutions (BI) Limited Dr Rick Adderley	United Kingdom
8	Technische Universitaet Graz Professor Dietrich Albert	Austria
9	Fraunhofer-Gesellschaft Zur Foerderung Der Angewandten Forschung E.V. Mr. Patrick Aichroft	Germany
10	Technische Universitaet Wien Assoc. Prof. Margit Pohl	Austria
11	ObjectSecurity Ltd Mr Rudolf Schriener	United Kingdom
12	Unabhaengiges Landeszentrum fuer Datenschutz Dr Marit Hansen	Germany
13	i-Intelligence Mr Chris Pallaris	Switzerland
14	Exipple Studio SL Mr German Leon	Spain
15	Lokale Politie Antwerpen	Belgium
16	Belgian Federal Police	Belgium
17	West Midlands Police	United Kingdom