Open Source Intelligence, Open Social Intelligence and Privacy by Design

Pompeu Casanovas [1,2]

[1] Institute of Law and Technology, Autonomous University of Barcelona,
08193-Barcelona, Spain, pompeu.casanovas@uab.cat
[2] Centre for Applied Social Research, Royal Melbourne Institute of Technology, Australia,
pompeu.casanovas@rmit.edu.au

Abstract. OSINT stands for *Open Source Intelligence,* (O)SI for (*Open) Social Intelligence*, PbD for *Privacy by Design*. The CAPER project has built an OSINT solution oriented to the prevention of organized crime. How to balance freedom and security? This position paper describes a way to embed the legal and ethical issues raised by the General Data Reform Package (GDRP) in Europe into this kind of surveillance platforms. It focuses on the indirect strategy to flesh out Privacy by Design principles (PbD) through Semantic Web Regulatory Models (SWRM). Institutional design, self-regulatory systems, and the possibility to build up a meta-level rule of law are discussed.

Keywords: CAPER, Open Source Intelligence (OSINT), Social Intelligence (SI), Semantic Web, Institutions, Semantic Web Regulatory Models (SWRM), Privacy by Design (PbD),

1 Preliminaries: the legal and political problem

There are many ways to face and conceptualize intelligence —individual, collective, swarm. etc. —to describe and research how it works or how to use it in courses of action. Since 2001 onwards this practical side has received a strong boost. The explosion of Internet, the wide use of protocols HTML, the speeding of the Semantic Web through W3C standards, are related to it. But the entrance in the new century through what it was called the *global terrorist threat* after September 11th was key to fund and promote new research programs for military use. Some of these programs are focused on Open Source Intelligence (OSINT).

The word is a bit misleading, because it is well known that Open Source (OS) has a venerable history in computing. There is also an ongoing discussion in legal theory on the role that OS plays in intellectual property, licenses, publishing and patents. But when applied to intelligence, OSINT does not refer only to the origin of the digital outcome but to the legal and political sphere of the community where the "intelligent" outcome is encapsulated, distributed, reused and transformed. What does it mean for a document, an image, a video to be qualified as OSINT? Basically that it is public domain or, better, *no man's land* domain, free to be grabbed and manipulated *for public reasons* by main representatives in nation-states —LEAs (Law Enforcement Agencies), Intelligence Services, State Agencies...

This paper deals with the relationships and differences between (Open) Social Intelligence (OSI) and Open Source Intelligence (OSINT). That is to say, with the ways to combine freedom and surveillance. This is at present one of the hottest topics of European legislation that it is worthwhile to tackle from a regulatory point of view.

The so-called General Data Reform Package (GDRP) is at stake. The new rules intend to put citizens back in control of their data, notably through: (i) a right to be forgotten (when you no longer want your data to be processed and there are no legitimate grounds for retaining it, the data will be deleted); (ii) easier access to your own data (a right to data portability to make easier to transfer personal data between service providers; (iii) putting citizens in control (requirement of explicit consent to process personal data), (iv) Privacy by Design (PbD) and Privacy by Default (PbD)—as they are becoming essential principles in EU Data Protection Rules [19].

The recent Opinion 28 released by the European Group on Ethics (EGE) of 20 May 2014 describes Ethics of Security and Surveillance Technologies [17]. The Opinion advances a set of sixteen concrete recommendations for the attention of the EU, member states, and a range of public and private stakeholders. It "*challenges the notion that 'security' and 'freedom' can be traded against one another*", and "*calls for a more nuanced approach, in which the proportionality and effectiveness of security and surveillance technologies are subject to rigorous assessment, and in which rights are prioritized rather than traded*". Certain core principles, such as human dignity, cannot be bartered with [18].

What does it exactly mean? In this position paper, I will show that replacing the mechanism of security as a *general exception* to rules by another approach in which other principles apply adds some complexity to the balance between freedom and security. I will follow up some ideas raised into the CAPER EU Project [10][1], stemming from some of the conclusions : (i) even in surveillance toolkits and serious security issues some feasible ways to bridge PbD principles and citizens' rights are possible; (ii) PbD can be broadly understood as a form of institutional design; (iii) ethics are starting to play a major role in such regulatory tasks.

2 A meta-level rule of law?

Let's start in reverse order and put some theoretical statements first. The problem of dealing with law is that *law* is not a well-defined field, where you can easily find its constituent elements and model them into rules and consequences. This is a discussion that has been lasting for centuries in the modern world. The French jurist Jacques Cujas (Cujacius, 1522-1590) defined the legal method as "the method of lack of method" in the 16c. Jeremy Bentham expressed the same feelings about *lawyer's cant*. Rules, norms, principles and values are expressed in natural language, and there is a real problem to face them analytically, because the same statute, article or concept might be *interpreted* in different ways any time they are instantiated in a ruling or in a decision-making process, and in fact they are.

[1] *Collaborative Information, Acquisition, Processing and Reporting for the Prevention of Organized Crime* (CAPER) http://www.fp7-caper.eu/

To put it crudely: law cannot be completely modelled. This is not saying that cannot be modelled. Only that cannot be modelled *up to the end*. This means at least two apparently opposing things: (i) there are objective limitations to formalize legal statements, (ii) the analyst is bounded to complete this missing part by settling some general framework *for his own sake*.

This can be like a leap into the dark, but it is most interesting to note that any practical decision or implementation of norms entails a theoretical ground. That is to say, from the epistemic point of view, the analyst is working at the same time through a constructing language and from a structuring meta-system for such a language. Models and meta-models come alike, and one of the interesting tasks is to make *explicit* the inner structure of the framework (the meta-model) legal models are made of or sorted out.

There are at least four kind of complexities related to: (i) semantic languages (and the explosion of data and metadata on the web), (ii) the socio-cognitive structure of individual and social mind (iii) the logical structure of nMAS (based on concepts like *agency*), (iv) institutional building within social ecosystems. To my purposes, I will focus on the latter one.

Sue Crawford and Elinor Ostrom defined *institutions* as formal and informal rules that are understood and used by a community [15]. Therefore, as advanced by legal realists in the thirties, institutions are not automatically what is written in formal rules. It is widely known that Vincent and Elinor Ostrom were looking for a dynamic and flexible framework expressible in a meta-model able to account for the fluidity of property rights (access, contribution, extraction, removal, exclusion, management/ participation, exclusion, alienation) and to overcome the static view of the "tragedy of the commons".

Their solution is generally referred to as the *just right* one, as balancing the aim of reducing the high costs associated with political solutions with that of ameliorating the absence of incentives to create solutions at all in the market-based approach [1].

Aligica and Boettke [2] have just highlighted that there is a deep social philosophy behind the Ostroms' approach. They developed in fact two frameworks: the *Institutional Analysis and Development* (IAD) framework as well as the *Diagnostic Ontological Social-Ecological Systems* (DOSES) framework. Thus, this philosophy holds in two different sides: (i) *polycentricity*, a notion that challenges two of the most common assumptions of political and economic sciences in the twentieth century (the monocentric vision of social order, and the “market” vs. “state” dichotomy); (ii) a view of *social order* seen as a knowledge and learning process within *social ecosystems* (factors engendering institutional order as a response to the challenges posed by them). But as the authors point out, there is no necessary connection linking the two perspectives involved in IAD and DOSES.

I will quote them at length, because Aligica and Boettke are fleshing out one of the more pervasive and striking problems that we have to face at present:

" To sum up, social order and its institutional dynamics are seen as shaped by (and operating under) the shadow of the ongoing tension between the “threat of chaos” and the “threat of tyranny.” Force and political constraint can be used as “instruments of tyranny as well as instruments to support productive and mutually advantageous relationships.” Could the problem of elemental asymmetry in the relationship between the “rulers” and the “ruled” be dealt in any way? Does, by its very nature, social order require that someone rules over society and cannot be held accountable to other members of society? Is it possible to conceptualize and organize the relationship between rulers and ruled so that rulers themselves are subject to a rule of law? In other words, could we design a “meta-level rule of law” where rulers themselves are subject to enforceable rules? Could we encapsulate it creating a climate dominated by deliberation and critical reason tempering the rulers and the application of force by checking and balancing them not only with the force of rules but also with reason and deliberation. The very effort of specifying such a solution is a means to appreciate the deep tensions that are involved in establishing a system of governance where both the *threat of chaos* and the *threat of tyranny* are circumvented. We are already in the territory of the *science and art of self-governance*.”

This possibility of "a meta-level rule of law" is crucial, because so far the mainstream of legal theory has not leaned on the understanding of decentralized boundaries, but on a hierarchical structure of norms, obligations and rights that are more based on the blueprint of normative or deontic languages than on the result of social and ecological analyses. How this meta-level rule could be built then?

It is worth noticing that classical 20 c. legal solutions to this problem do not apply here. Kelsenian *Grundnorm*, Hartian *recognition rule* or the assumption of selective *sources of law* to set a principle of legality —Alf Ross' solution for the grounding of *national* statutes— cannot constitute potential answers any more, as from the ecosystems perspective law does not encompass the whole problem, but only one of its dimensions. A similar problem is faced in agreement technologies, when Online Dispute Resolution (ODR), nMAS and crowdsourcing enhance aggregated collective information and social intelligence processes [8].

Besides, legal theory approaches lean on the (not always assumed) *situated perspective* taken by lawyers, jurists and rule-makers in conflictive environments. The Polish logician Jerzy Wróblewski put it quite clearly when he stated that lawyers *make* the law of the land, and therefore the *language of law* is intertwined with the *language of lawyers*. Legal design is to a great extent political design too. Let's face the problem from another side.

3 Open Source Intelligence (OSINT) and Social Intelligence (OSI)

OSINT, is usually defined as intelligence collected from open sources. There is no homogeneous approach to this concept, depending on the field, purposes and actions in which it is used. Intelligence Services refer to it as "unclassified information that has been deliberately discovered (...) to a select audience", i.e. military uses [30]. Reports for the US Congress are quite clear about this: "A consensus now exists that OSINT must be systematically collected and should constitute an essential component of analytical products" [5]. This is especially felt when working on the edges of law, balancing freedom and security, surveillance and fundamental rights. General Michael Hayden, former director of the NSA and the CIA, furnishes an extreme example. He conspicuously stated in a recent debate with David Cole at John Hopkins University: *We kill people based on metadata* [14].

But OSINT is considered also for other unrelated aims a cluster of tools to browse the web, aggregate information, and getting reliable profiles from websites, blogs, social networks, and other public settings. From this broader point of view, it may be defined synthetically as "the retrieval, extraction and analysis of information from publicly available sources" [4]. This approach is taken by many to get, structure and manage information in a broad array of social domains —media [6], education [24], business [20], disaster management [3].

The former is a definition of the concept referring to functions being performed by a computer system —retrieval, extraction and analysis of information. It is ostensive in nature, offering a descriptive meaning. Could OSINT somehow be related to (Open) Social Intelligence (O)SI)?

Only in a superficial way. Both concepts have an operational side and denote the circulation and transformation of non-structured information into structured information on the web. In their history of the concept, Glassman and Klang offer a communicative and cultural approach —"the Web as an extension of mind", OSINT as the interface between *fluid intelligence* and *crystallized intelligence* [3].

If this is so, the field, methodology and theory of Social Intelligence comprehends what is referred by OSINT, as the social mind is faced as a set of social affordances that can be represented, described and reproduced computationally as *inner* mechanisms, as social *artifacts* performing a collective work [11]. Social Intelligence focuses on the human/machine coordination of *artificial socio-cognitive technical systems*, assuming that they interact in a shared web-mediated space with aims, purposes, intentions, etc. and are amenable to models *and* meta-models from a theoretical point of view [27].

If the concept of *OSINT tools or platforms* is used to describe the operational functionalities of a computational system, this use should be embedded into a conceptually broader set of notions to be effective. In artificial socio-cognitive systems "rationality is based on the model that agents have of the other agents in the system" [28]. This epistemic assumption is not necessary in OSINT systems, more pragmatically oriented and centered on visual analytics and on the interface between intra and inter-organizational teams.

Let's face this problem stemming from a different side —which meta-model would be needed to build the institutional design of civil rights protections (the balance between freedom and security)?

4 Privacy by Design (PbD)

For some time now, the main concepts of Privacy by Design (PbD) —and Data Protection by Design and by Default— have been widely spread over computer science and legal research communities [12]. This conceptual body intends to develop the Principles of Fair Information Practices (FIPs)[2] that follow (i) from the Alan

[2] 1. Openess and Transparency, 2. Individual Participation. 3. Collection Limitation, 4. Data Quality, 5. Use Limitation, 6. Reasonable Security. 7. Accountability.

Westin tradition in private law[3], (ii) and the technological idea of a meta-layer to manage and secure the identity of users on the web set by the Microsoft architect Kim Cameron [7].

Ann Cavoukian has recently asserted that "*it is not true that privacy and security are mutually opposing*", and that big and smart data "*proactively builds privacy and security in*" [12]. It might be true, but it is not evident in the fight against organized crime. Both in the military or humanitarian fields, to be effective OSINT tools have been designed just for what they should be controlled: spotting as much as possible and getting personal information about individuals and organizations.

Bert-Jaap Koops, Jaap-Henk Hoepman [23] and Ronald Leenes [25] [26] experienced this void on the sidelines of law and technology when they faced the problem of modelling the protections of General Data Reform Package into OSINT platforms.[4] As might be expected, they found that privacy regulations cannot be hardcoded —"'privacy by design' should not be interpreted as trying to achieve rule compliance by techno-regulation. Instead, fostering the right mindset of those responsible for developing and running data processing systems may prove to be more productive. Therefore, in terms of the regulatory tool-box, privacy by design should be approached less from a 'code' perspective, *but rather from the perspective of 'communication' strategies* [emphasis added]".

Regarding the analysis, I am going along to the authors' guidelines, but perhaps another conclusion could be drawn as well from these limitations. There are other possibilities to embed PbD into surveillance platforms, albeit indirectly, i.e. adding theoretical views not thinking of *techno-regulation* but of what law means when constructed through technological means. It is properly legal theory what could be worked out from the perspective of self-governance and socio-cognitive artificial systems.

E,g. CAPER is a system comprising a platform whose main functionalities are accorded to OSINT features: (i) implementing a framework to perform the task of connecting multiple data sources with multiple visualization techniques via a standardized data interface, including support for data-mining components; (ii) enabling a quick import of data types from disparate data sources in order to improve the ability of different LEAs to work collaboratively; (iii) supporting pattern discovery, documentation and reuse, thus increasing progressively detection capabilities. The architecture design has four components: (i) Data harvesting (knowledge acquisition: data gathering), (ii) analysis (content processing), (iii) semantic storage and retrieval, (iv) and advanced visualization and visual analytics of data. For sake of clarity, Fig. 1 shows the interaction and workflow between databases.

[3] These historical origins must still be retraced and reconstructed carefully. I am grateful to Graham Greenleaf for this observation.

[4] VIRTUOSO (*Versatile InfoRmation Toolkit for end-Users oriented Open-Sources explOitations)*, http://www.virtuoso.eu/ .

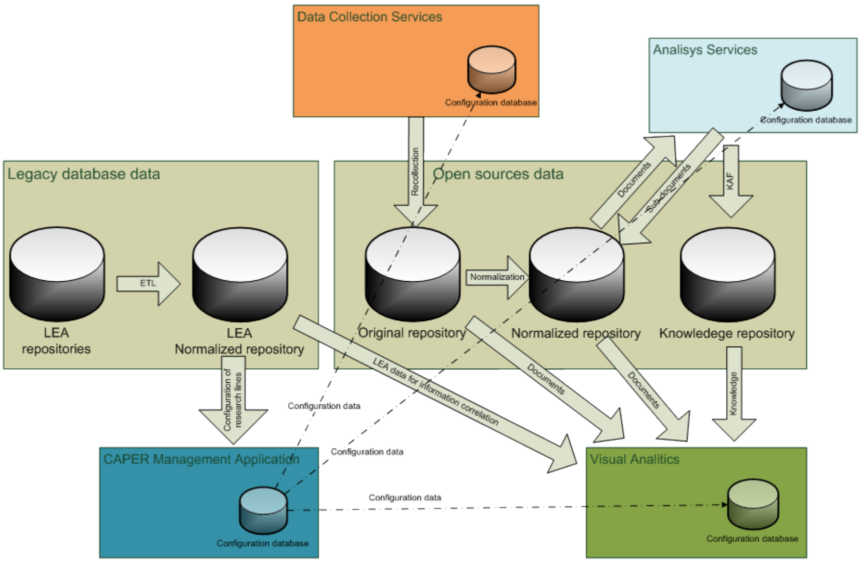

Figure 1. CAPER Databases Overview.

We explored several related strategies that constitute an *indirect* approach to PbD principles; and five different strategies were designed [10]:

1. CAPER workflow is addressed in fact to four different LEA´s analysts: (i) The *Generic Analys*t (GA) (ii) the *Advanced Analyst* (LEA-AA) (iii) the *System Administrator*, (iv) LEA's External User (LEU).
2. Well-defined scenarios are extracted from the experience of managing specific types of crimes. CAPER tools operate only within the investigation conducted by LEAs, helping them to better define the lines of research, but avoiding any automated conceptualization of them.
3. Well-defined module interdependencies are drawn in advance. CAPER crawling system is sustained by three modules: (i) crawler by keyboard, (ii) by URL, (iii) by URL focusing on keyboards. But the crawler is able to convert images and videos metadata into allowed mimetypes required by the *Visual Analytics* module (VA). Multi-lingual semantics is added to the whole process as well.
4. Two different kind of ontologies have been built. The first one is a Multi-lingual Crime Ontology (MCO) for 13 languages, including Hebrew and Arabic, with a proof of concept on drugs (346 nodes). MCO works according to the country legislation (possession of drugs is a crime in UK, but not in Spain e.g.).
5. The second one is properly a legal ontology, focused on European LEAs Interoperability (ELIO). ELIO has been built with the purpose of improving the acquirement and sharing of information between European LEAs [22].

This pack of actions constitutes a warrant for citizens' rights. Design means *institutional design* as well. The notion of *institutional-Semantic Web Regulatory Model* (i-SWRM) leans on this assumption: a self-regulatory model embeds the dimension of PbD into a technological environment than can be represented as a social ecosystem [8]. This is similar (with some differences) to the framework set in [25] [26] and specifically in [23].

Hoepman's PbD strategies model focuses on the inner structure of the modeling, signaling several points into a general framework for privacy (or data protection) closed managerial system. This is consistent with the idea of concentrating the effort onto the interpretation of the law, putting aside the specific problems, risk scenarios, and asymmetric multilayered governance of OSINT platforms, end-users and LEA. Conversely, i-SWRMs and specifically the regulatory model designed to regulate the CAPER workflow system (CRM), are more focused on LEA's inner and outer relationships. The social ecosystem centered on the specific data that users are processing and "living by" can be outlined as a simple scheme described in advance (see fig. 2).

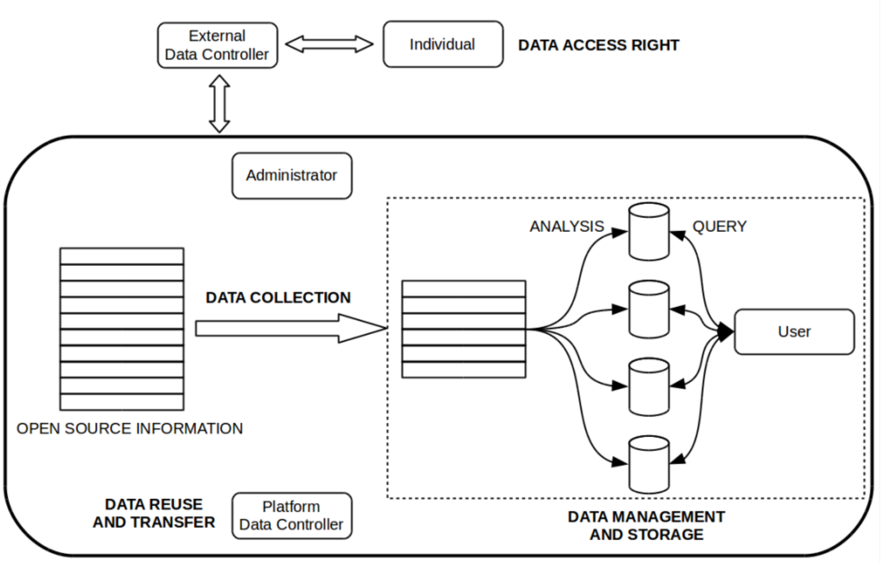

Figure 2. CAPER regulatory scheme [22].

Affordances can be plotted on the CAPER workflow, along with data protection rules. However, 9 out of the 23 rules, could not be situated because they don't apply to the information process, but to LEA's behavior (analysts, controller, administrator). This holds, e.g. for a positive obligation such as "Every LEA should perform a specific Privacy Impact Assessment (PIA) according to the general framework offered by the CAPER Regulatory Model (CRM)", a general prohibition as "No automated classification of suspects, victims and witnesses can be inferred from CAPER results", and for specific obligations such as "The alleged reasons to deny access should be open to external supervision. The external supervisory authority should have free access to documents justifying the refusal. A short time-span of three months to give an answer to a previous request of access should be implemented".

5 The role of normative and institutional Semantic Web Regulatory Models (n-SWRM, i-SWRM)

Let's get back to Aligika's and Boettke's [2] main questioning: Would it be possible to conceptualize and organize the relationship between rulers and ruled so that rulers themselves are subject to a rule of law? In other words, could we design a “meta-level rule of law” where rulers themselves are subject to enforceable rules?

Semantic Web Regulatory Models (SWRM) co-organize the conceptual architecture of (enforceable) hard law and (non-enforceable) soft law, best practices and ethics. Compliance with norms is important, but it is not enough. Reaching a sustainable behavioral model is equally important. The validity of the system is shown through the emerging independent axis of *institutional strengthening*. This approach presents the additional advantage of being measurable.

E.g., in the CAPER example dialogue with LEA and security experts is crucial to understand where the problems are and why, and to let LEA's investigators participate into the regulatory process. At the same time, control is exerted because binding norms apply as well. E.g. the need for an internal and external DP controller (competent DP authorities) and the obligation to set a strict log file to keep records to sustain the accountability of the whole system.

So, the Caper Regulatory Model (CRM) lying behind the actions taken intends to bridge negotiations of social agents with the normative requirements and conditions of the rule of law (reinterpreted from this broader standpoint). This is why it can be implemented among LEA's organizations and embedded into the CAPER system to regulate the use of the platform. CRM is an example of i-SWRM.

There are two types of SWRM [8]. *Normative-SWRMs* (n-SWRMs) use RDF, RuleML and computer versions of rights, duties and obligations. They may lean on the use and reuse of nested ontologies or "ontological patterns". Digital Rights Management (DRM), Rights Expression Languages (REL) are quite useful to represent legal licenses, intellectual property rights, or patents as data and metadata to be searched, tracked or managed in a global way on the Internet. Creative Commons is a well known example for using REL to express licenses. Open Digital Rights Language (ODRL) initiative constitutes another example. Therefore, *end-users and systems are linked through the same tool that is being used to manage and apply the modeled legal knowledge*.

Institutional-SWRM (i-SWRM) are focused on the relationship of end-users with their own organizations. Inner coordination among electronic agents, outer interface with human (collective) agents, and their dynamic interaction within different types of scenarios and real settings are key. They can be applied to regulatory systems with multiple normative sources and human-machine interactions between organizations, companies and administrations. Thus, their conceptual scheme is linked with legal pluralism and with existing models of asymmetric multi-layered and networked governance. Those are conceptual constructs compatible with Ostrom's social philosophy —polycentricism and social ecosystems— because their center of gravity lie on their dynamic social bonds. *End-users and systems are connected through the social and legal bonds that externally link them*.

We could now reframe the original questions we started with. How are i-SWRS and n-SWRS related? How could they work together to frame this *meta-level rule of law*? Which self-regulatory institutions could be based on such a model?

If we start finding reasonable answers perhaps we will be able to circumvent the dichotomy between Ostrom's particular Scylla and Charibdis —the threats of chaos and tyranny for the 21c.

Acknowledgments. This research has been funded by the F7 EU Project *Collaborative information, Acquisition, Processing, Exploitation and Reporting for the prevention of organised crime* (CAPER) —Grant Agreement 261712—; and partially by the National Project *Crowdsourcing*, DER2012-39492-C02-01.

References

1. Aldrich, J.H.: Elinor Ostrom and the "just right" solution, Public Choice 143, pp. 269-273 (2010) DOI 10.1007/s11127-010-9630-9
2. Aligica, P.D., Boettke, P.: The Two Social Philosophies of Ostroms' Institutionalism, The Policy Studies Journal, 39,1, pp. 29-49 (2011)
3. Backfried, G., Schmidt, C., Pfeiffer, M., Quirchmayr, G., Markus Glanzer, M., Rainer, K.: Open Source Intelligence in Disaster Management. 2012 European Intelligence and Security Informatics Conference, EISIC, IEEE Computer Society, pp. 254-258 (2012)
4. Best, C.: Open Source Intelligence, in F. Fogelmann-Soulié et al.(Eds.), Mining Massive Data Sets for Security: Advances in Data Mining, Search, Social Networks and Text Mining, and Their Applications to Security 19 , Amsterdam, IOS Press, 2008, pp. 331-344.
5. Best, R., Cumming, A.: Open Source Intelligence (OSINT): Issues for Congress, *CRS Report for Congress*, Order Code RL34270, Updated January 28 (2008)
6. Bradbury, D.: In plain view: Open Source Intelligence, Computer Fraud & Security 4**,** pp. 5-9 **(**2011)
7. Cameron, K.: The Laws of Identity …as of 5/11/2005. Microsoft Corporation, http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf
8. Casanovas, P.: Agreement and Relational Justice: A Perspective from Philosophy and Sociology of Law, Sascha Ossowski (Ed.) Agreement Technologies, LGTS n. 8, Springer Verlag, Dordrecht, Heidelberg, pp. 19-42 (2013)
9. Casanovas, P.: Semantic Web Regulatory Models: Why Ethics Matter, Philosophy & Technology, DOI 10.1007/s13347-014-0170-y. 27, 2 (2014)
10. Casanovas, P., Arraiza, J., Melero, F., González-Conejero, J., Molcho, G., Cuadros, M. Fighting Organized Crime Through Open Source Intelligence: Regulatory Strategies of the CAPER Project. Submitted at JURIX 14, Cracow (2014)
11. Castelfranchi, C.: Minds as Social Institutions, Phenomenology and Cognitive Science DOI 10.1007/s11097-013-9324-0 (2013)
12. Cavoukian, A.: Privacy by Design. The 7 Foundational Principles. Implementation and Mapping of Fair information Practices. Information and Privacy Commissioner, Ontario,

Canada, (2010) http://www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/

13. Cavoukian, A.: Privacy by Design, IEEE Technology and Society Magazine, DOI 10.1109/MTS.2012.2225459, pp. 18-19 (2012)
14. Cole, D.: 'We kill people based on metadata', New York Review of Books, 10th May (2014) http://www.nybooks.com/blogs/nyrblog/2014/may/10/we-kill-people-based-metadata/?insrc=wbll
15. Crawford, S., Ostrom, E.: A Grammar of Institutions, in E. Ostrom (Ed.) Understanding Institutional Diversity, pp. 137-174. Princeton University Press, New Jersey (2005)
16. Gangemi, A.: Ontology semantic web patterns for semantic web content. Y. Gil et al. (Eds.), ISWC 2005, LNCS 3729, pp. 262–276 (2005)
17. EGE: Ethics of Security and Surveillance Technologies, Opinion no. 28 of the European Group on Ethics in Science and new Technologies, Brussels, 20 May 2014, http://ec.europa.eu/bepa/european-group-ethics/docs/publications/ege_opinion_28_ethics_security_surveillance_technologies.pdf
18. EGE: Press Release on the EGE Opinion 28, of 20 May 2014. http://ec.europa.eu/bepa/european-group-ethics/docs/publications/press_release_ege_opinion_28_.pdf
19. EU Commission: Progress on EU data protection reform now irreversible following European Parliament vote European Commission - MEMO/14/186 12/03/2014, http://europa.eu/rapid/press-release_MEMO-14-186_en.htm
20. Fleisher, C. OSINT: Its Implications for Business/CompetitiveIntelligence Analysis and Analysts, OSINT: Its Implications for Business/Competitive Intelligence Analysis and Analysts. Inteligencia y Seguridad , 4, pp. 115-141 (2008)
21. Glassman, M., Kang, M.J.: Intelligence in the internet age: The emergence and evolution of Open Source Intelligence (OSINT), Computers in Human Behavior 28, p p. 673-682 (2012)
22. González-Conejero, J., Varela-Figueroa, R., Muñoz-Gómez, J., Teodoro, E.: Organized Crime Structure modelling for European Law Enforcement Agencies Interoperability through Ontologies, P. Casanovas, U. Pagallo, M. Palmirani, G.Sartor Ed.) *AICOL 2013*, LNAI, Heidelberg, Dordrecht, Springer, 2014 (forthcoming)
23. Hoepman, J-H: Privacy Design Strategies (extended abstract), N. Cuppens-Boulahia et al. (Eds.), ICT Systems Security and Privacy Protection - 29th IFIP TC 11 International Conference, SEC 2014, Marrakech, Morocco, June 2-4, 2014. Proceedings. Springer 2014 IFIP Advances in Information and Communication Technology, pp. 446-459 (2014)
24. Kim, Y.,Glassman, M., Bartholomew, M., Hur, E.H.: Creating an educational context for Open Source Intelligence: The development of Internet self-efficacy through a blogcentric course, Computers & Education 69, pp. 332-342 (2013)
25. Koops, B.J., Hoepman, J.H., Leenes, R.: Open-source intelligence and privacy by design, Computer Law & Security Review 29, pp. 676-688 (2013)
26. Koops, B-J, Leenes, R.: Privacy regulation cannot be hardcoded. A critical comment on the ‘privacy by design’ provision in data-protection law, International Review of Law, Computers & Technology (2013) DOI: 10.1080/13600869.2013.801589.
27. Noriega, P., Padget, J., Verhagen, H., d'Inverno, M.: The Challenge of Artificial Socio-Cognitive Systems, in: AMMAS 14’ Proceedings at: http://aamas2014.lip6.fr/proceedings/workshops/AAMAS2014-W22/p12.pdf.
28. Noriega, P., d'Inverno, M.: Crowd-Based Socio-Cognitive Systems, in Crowd Intelligence: Foundations, Methods and Practices. European Network for Social Intelligence, Barcelona, January 2014, ed. M. Poblet, P. Noriega, E. Plaza (eds.) http://ceur-ws.org/Vol-1148/CROWD2014

29. Ostrom, E.: Institutional Analysis and Development. Micro Workshop in Political Theory and Political Analysis, Proceedings f the Policy Studies Organization, New series 9, pp. 851-878 (2010) http://www.ipsonet.org/proceedings/category/volumes/2010/no-9/
30. Steele, R.D: Open Source Intelligence, Loch Johnson (Ed.), Handbook of Intelligence Studies, pp. 129-147, Routledge, New York (2007)