SECURITY AND
HUMAN RIGHTS
MONITOR

Information Management professionals working for intelligence organizations: ethics and deontology implications

Diego Navarro Bonilla[1]*
Associate Professor of Archival Science, Library and Information Sciences Dpt., University Carlos III of Madrid (UC3M, Spain)
Founder, Institute of Research on Intelligence for Security and Defence (UC3M)

dnavarro@bib.uc3m.es

DOI: 10.1163/18750230-02404005

[1] * The author would like to thank Prof. Miguel Ángel Esteban (University of Zaragoza) and Prof. José Manuel Ugarte (Univ. of Buenos Aires) for their extremely useful comments.

Abstract

Archive and information management experts trained in library science programs are ideal candidates for jobs in intelligence organizations. Their skills, abilities and knowledge are frequently required in at least two well-defined areas: open source information gathering and records management/archival organisation. Under the general overview of the debate between “big data vs. big narrative” this article focuses on the ethical challenges that affect this community of information professionals. As a key component of the so-called “intelligence culture”, it will be also underlined the need for intensifying from our university classrooms the ethical dimension of information exploitation for security and defence purposes. The role played by these information profiles involved in multiple phases of the intelligence production process must be based not only on efficiency and efficacy criteria but also on deontology principles whose benefits are the fortification of democratic practice by intelligence services working in strong legal frameworks designed to guarantee fundamental rights.

Keywords

records information Managers; intelligence production; deontological codes; big data; fundamental rights

Introduction and aim

The 1673 edition of Jesuit Athanasius Kircher’s (ca. 1603-1680) Phonurgia Nova (Universa Sonorum Natura… per occultioris ingenii machinamenta) described a curious invention. Its Liber I sectio VII included an engraving showing huge secret apparatuses that would enable a ruler to overhear conversations in streets, squares, corridors in his own court and even in secretaries’ and foreign princes’ cabinets. Hidden in the walls of buildings, one end would pick up voices from the outside and transmit them to the other, located inside a special room. Such seventeenth-century acoustic espionage might well be regarded as a precursor, a kind of protoSIGINT.

Whether or not Kircher’s prototypes ever actually got any farther than the drawing board, they constitute an historical example of an aspiration as old as humanity. Limited only by the technology available at any given time, rulers desire omniscience, for the greater the amount of information and the larger the number of secrets indiscriminately and massively unveiled, the more absolute is their power. The hazards involved in the excessive accumulation of information or knowledge to be analysed and processed are consequently not only a concern today. Rather, as Marc Andrejevic[2] points out in his new book, Infoglut, its roots date back to Early Modern Europe, as masterfully discussed by Ann Blair in her now classic Too much to know.[3]

Centuries later, those large “ears” strategically positioned in the squares, corridors and cabinets of the early modern State may look like a naive attempt to decipher secrets and monitor conversations on a universal scale. Nonetheless, the spirit of that endeavour is timeless, presently adopting the form of multiple international ears deployed in intelligence stations designed for extensive signal interception. Public awareness of such facilities was vague at best until their raw reality and scope were laid bare by Snowden’s revelations about the NSA’s and other international agencies’ activities. The widespread use of mobile devices by individuals and the ethical issues associated with the privacy of the data generated and transmitted, constituting what Roux and Falgoust called “extended cognition”, continue to be a matter of growing academic

[2] Marc Andrejevic, Infoglut: How Too Much Information Is Changing the Way We Think and Know, Taylor and Francis, 2013.

[3] Ann Blair, Too Much to Know: Managing Scholarly Information before the Modern Age, Yale University Press, 2011.

and media concern.[4] The term “big data”, with its deep and troubling Orwellian connotations, was adopted by the media as the new buzzword in the summer of 2013. For some time now, a day rarely goes by without a headline or two on the matter in the media. Specialised monographs, among them a book by Mayer-Schönberger and Cukier[5] that has been translated into a number of languages, attempt to furnish the public at large with a better grasp of issues that stand at the core of the controversy around the activities conducted by intelligence services today. If, as these authors contend, the practice of big data constitutes a revolution, that revolution would need to be sited on the map of innovations and changes in the intelligence paradigm[6] charted over the last twenty years by the so-called “revolution in intelligence affairs” described by Deborah Barger in a pioneering study.[7]

Further to the many dilemmas posed around obtaining OSINF, in this article I focus on the deontological dimension of information handling, the acquisition of huge volumes of data and their transformation into sources of knowledge. My premise is that if OSINF “requires more (State) accountability” as Roux and Falgoust correctly contend, (political, economic and judicial) improvement of controls over intelligence activity is required to strengthen the guarantee of fundamental rights in democratic systems.[8] However, that is not the only area where action is needed. The ethics and deontology of information and documentation professionals who may ultimately work in intelligence services or their collaborating companies must also be reinforced from our university classrooms. In this article I will discuss why the three components of the training and formation programmes of the intelligence practitioners require much more than efficiency and efficacy as a result of skills, abilities and knowledge. Intensifying the ethical dimension of information management is also a component of so-called “intelligence culture”, one of whose benefits is the fortification of democratic practice by intelligence services working in legal frameworks designed to guarantee such rights.

In pursuit of total data

Those early modern designs and prototypes minded by Kircher are now, of course, a far cry from today’s devices for espionage en masse. And yet they were a prelude to modern and contemporary powers’ technological endeavour to acquire systems and mechanisms for monitoring communications in the framework of programmes with large-scale, comprehensive and planetary aspirations. This constant pursuit has intensified since 9-11, as attested to by the objectives and programmes sponsored by agencies such as DARPA (Defense Advanced Research Projects Agency) and DISA (Defense Information Systems Agency): Total Information Awareness Office inspired by J. Poindexter (2002), Information Processing Technology, Information Exploitation Office, etc. Alone or in conjunction with outside companies such as In-Q-tel.com associated with the intelligence community’s agencies, they have aspired to widespread, global and effective information harnessing and fostered the institution of a new generation of software and hardware tools applicable to national security. Electronic communications monitoring, the retrieval and control of millions of data items through data mining or machine translation, bio-surveillance or the application of tools involved in the automatic processing of natural language are only a few of the many areas of priority interest. R&D

[4] Brian Roux and Michael Falgoust, “Information ethics in the context of smart devices”, Ethics and Information Technology, September 2013, 15: 3, pp. 183-194.

[5] Viktor Mayer-Schönberger y Kenneth Cukier, Big Data: a Revolution that will Transform how we Live, Work and Think, Houghton Mifflin Harcourt, 2013.

[6] William Lahneman, Keeping U.S Intelligence Effective: The Need for a Revolution in Intelligence Affairs, Maryland, Scarecrow, 2011.

[7] Deborah Barger, Toward a Revolution in Intelligence Affairs, Santa Mónica, Rand Corporation, 2005.

[8] Peter Gill, Policing Politics: Security Intelligence and the Liberal Democratic State, Frank Cass, London, 1994. José Manuel Ugarte, El control público de la actividad de inteligencia en América Latina, Buenos Aires, CICCUS, 2012.

programmes conducive to the exploitation of sources of information across a wide range of formats and typologies would provide support for the controversial “preventive selfdefence” doctrine developed by the Department of Defense under the leadership of Donald Rumsfeld.

This is the backdrop against which the media have spotlighted the role and responsibility attributed first to the NSA and subsequently to many other intelligence services. A thoughtful study is in order of the ethical implications of the tasks performed by employees rendering their services not only in governmental intelligence agencies, but also in competitive and business intelligence units or companies and agencies to which such services are outsourced. The community of information and documentation professionals trained in library and information science schools and departments is of particular interest in this regard. Experts in handling open source information (OSINF), they are not at all unfamiliar with the term “metadata management”. They routinely use EAD/EAC/MARC and similar standards. They are conversant with metadata standardisation, monitoring, and management initiatives applied to bibliographic and scientific information (Dublin Core Metadata Initiative or Preservation Metadata: Implementation Strategies (PREMIS), Metadata Object Description Schema (MODS)). Moreover, they must continually update their skills to rise to the challenges posed by descriptive metadata linked to open data in the semantic web environment as well as by open data and access to public information in keeping with the provisions of current laws on transparency such as the recently approved legislation in Spain Law 9/2013, Dec. 9th, on transparency, access to public information and good government.[9] They are similarly skilled in many other information management and knowledge production tasks, phases and sub-routines involved in intelligence, from the formulation of ontologies within the semantic web to information visualisation. For that reason, although the development of metadata formats has traditionally been driven by multimedia techniques and the semantic web, the application of metadata management to intelligence, security and defence has become an enormously suggestive endeavour. In short, these professionals’ contact with millions of data items across a wide spectrum of origins positions them on the threshold of data mining. The obvious inter-relationships among the efficient and accurate gathering and processing of information and its transformation into knowledge for State security and defence has been seen, on the other hand, as a new academic research field under the broad label of the so-called “intelligence culture”.[10] This, to a certain degree, is the general “information landscape” and the pursuit of opportunities “to assert the value of information professionals and the intelligence community” recently analysed by Arno Reuser.[11]

The eternal dichotomy between security and freedom/privacy casts uncertainty over this community of information professionals. Their codes of ethics provide stable reinforcement for countering the abuse and deviation from accepted practice and established principles that may arise in the performance of the many phases, tasks and routines involved in intelligence production: from the identification of open data repositories to the design of information search strategies or social network monitoring for intelligence purposes. “The use of OSINF for intelligence purposes has real life consequences”. The authors of that

[9] Eva María Méndez Rodríguez, Jane Greenberg, “Linked data for open vocabularies and HIVE’s global framework”, El profesional de la información, 21: 3 (2012), pp. 236-244. Special issue devoted to Knowledge Management.

[10] Miguel Ángel Esteban Navarro and Diego Navarro Bonilla, “Gestión del conocimiento y servicios de inteligencia: la dimensión estratégica de la información”, El Profesional de la Información, Julio-agosto 2004, vol. 12, núm. 4, pp. 269-281. H. Minas, “Can the open source intelligence emerge as an indispensable discipline for the intelligence community in the 21st century?”, RIEAS (Research Institute for European and American Studies) Research Paper, No. 139, (January 2010); http://bit.ly/17OmZFu.

[11] Arno Reuser, “Trends in the Current Information Landscape and Their Significance for Researchers”, Online Searcher (Jan.-Feb. 2013), pp. 51-55.

assertion, Eijkman and Weggemans, wrote a brilliant article analysing the need to generate a specific legal framework for OSINT, to broaden accountability schemes and to enhance transparency in the use of and capitalisation on open information resources. "The use of OSINT for safety and security purposes is a reality, but (re) assessing State accountability is necessary for its legitimate use by security and intelligence agencies and the police".[12]

Defining the dilemma

Fairly frequently, during or after seminars, workshops, conferences and classes devoted to the improvement of professionals' OSINF search and acquisition skills and their ability to transform such data and information into new knowledge, the same situation has emerged. I have been hesitantly approached by one or several young students drawn by the inevitable appeal and glamour of intelligence activities, invariably wanting to know how they can find employment with the Spanish intelligence service. What no one has asked me to date is how they should deal with the professional dilemma posed by the need to balance fundamental rights, on the one hand, and the processing of large volumes of personal data in the interests of national security or defence, on the other. Intelligence is subject to a legal and regulatory framework. In countries such as Spain the legislation in place for intelligence services apparently guarantees citizens' rights. From the legal perspective, then, theoretically and ideally this dilemma should never arise because, as the Secretary of State in charge of Spanish intelligence claimed in a Commission on Official Secrets hearing (November 2013), "in Spain the secret services act within the framework of legal guarantees".

Barely one month ago, Carlos III University of Madrid's information and documentation graduate students defended their end-of-course dissertations. One of the assessment criteria was the inclusion or otherwise of their "civil, ethical and deontological commitment". Explicit mention of that commitment in the papers authored by future librarians, archivists or information and documentation specialists raised the final mark. Conversely, the lack of commitment or an explicit mention of the ethical dimension of their research was assessed adversely. Codes of conduct in place for many years and endorsed by professional associations, chartered institutes and international bodies such as IFLA/ICA and national organisations such as FESABID/COBDC/SEDIC, as well as by the American Library Association, the Society of American Archivists and the Archives and Records Association (UK/Ireland) to name but a few, exhibit a clear determination to respect ethical principles, values and rules in the practice of the information professions.[13] Ethics in information is by no means a new or scantly studied issue.[14]

It is hardly a trivial question, however, insofar as indications of the more than likely violation of codes of conduct by professionals in the name of national security have surfaced in and around the Snowden case. By way of an example, a report directly and clearly entitled Ethics abandoned: Medical Professionalism and Detainee Abuse in the War on Terror (Institute on Medicine as a Profession/Open Society Foundation)[15]

[12] Quirine Eijkman and Daan Weggemans, "Open Source Intelligence and Privacy Dilemmas: Is It Time to Reassess State Accountability", Security and Human Rights, 4 (2012), pp. 285-296.

[13] IFLA: International Federation of Library Associations; ICA: International Council on Archives; SEDIC: Asociación Española de Información y Documentación; FESABID: Federación Española de Sociedades de Archivística, Biblioteconomía, Documentación y Museística; COBDC: Colegio Oficial de Bibliotecarios-Documentalistas de Cataluña.

[14] Robert Hauptman, Ethical challenges in librarianship, Phoenix, Oryx Press, 1988. Barbara J. Kostrewski, Charles Oppenheim, "Ethics in information science", Journal of information science, 1: 5 (Jan. 1980), pp. 277-283. Richard O. Mason, Florence M. Mason, Mary J. Culnan, Ethics of information management, Thousand Oaks, CA: Sage Publications, 1995.

[15] Ethics abandoned: Medical Professionalism and Detainee Abuse in the War on Terror (A task force report funded by Institute on Medicine as a Profession/Open Society Foundation www.imapny.org/File%20Library/Documents/IMAP-EthicsTextFinal2.pdf.

censures the probable involvement of doctors and psychologists working for the Pentagon or the CIA who could have contributed to the preparation and implementation of interrogations, torture and demeaning treatment of terrorist suspects. The Senate Intelligence Committee has been asked to investigate the veracity and scope of the study's conclusions.

Library and information professionals in intelligence positions

Can a professional trained to manage information or exploit open information resources to contribute to OSINT become a whistleblower? Much has been said and written about ethics in intelligence and considerable effort has been made to try to harmonise what some authors consider an oxymoron.[16] Studies such as those conducted by the International Intelligence Ethics Association or Jan Goldman at the head of the International Journal of Intelligence Ethics provide guidelines for the ethical dimension of intelligence tasks. Nonetheless, in Spain, at least, I have not seen that perspective discussed at any length in recent commentaries or the news.

Table 1. Codes of ethics in effect in the professional societies of librarians, archivistsand information managers.

Codes of Ethics for Library, Archives and Information Management Professionals	
IFLA Code of Ethics for Librarians and other Information Workers. 12 August 2012.	3. Privacy, secrecy and transparency Librarians and other information workers respect personal privacy, and the protection of personal data, necessarily shared between individuals and institutions. The relationship between the library and the user is one of confidentiality and librarians and other information workers will take appropriate measures to ensure that user data is not shared beyond the original transaction. Librarians and other information workers support and participate in transparency so that the workings of government, administration and business are opened to the scrutiny of the general public. They also recognise that it is in the public interest that misconduct, corruption and crime be exposed by what constitutes breaches of confidentiality by so-called 'whistleblowers'.
International Council on Archives, Code of Ethics [Adopted by the General Assembly in its 13th session in Beijing, China on 6 September 1996]	7. Archivists should respect both access and privacy, and act within the boundaries of relevant legislation. Archivists should take care that corporate and personal privacy as well as national security are protected without destroying information, especially in the case of electronic records where updating and erasure are common practice. They must respect the privacy of individuals who created or are the subjects of records, especially those who had no voice in the use or disposition of the materials. 8. Archivists must refrain from activities which might prejudice their professional integrity, objectivity and impartiality. They should avoid activities that could create in the public mind the appearance of a conflict of interest. […] Archivists should not allow people outside the profession to interfere in their practice and obligations.

[16] Allison Shelton, "Framing the Oxymoron: A New Paradigm for Intelligence Ethics", Intelligence and National Security, 26: 1 (2011), pp. 23-45.

Codes of Ethics for Library, Archives and Information Management Professionals	
Código Deontológico (Code of Conduct), SEDIC (10.03.2013)	4. Privacy and confidentiality. (Members) must guarantee professional secrecy in the performance of their duties to protect the confidentiality of information and documentation service users' personal data, subject only to the limitations laid down by law. They must seek to ensure and respect professional and family privacy and personal image in the performance of their duties.
Archives and Records Association (UK/Ireland) Code of Conduct	Members should respect both access and privacy, and act within the boundaries of relevant legislation. Members should take care that corporate and personal privacy as well as national security are protected without destroying information, especially in the case of electronic records where updating and erasureare common practice. They must respect the privacy of individuals who created or are the subjects of records, especially those who had no voice in the use or disposition of the materials. Members will seek to strike an appropriate balance between rights of access and privacy.
Código Deontológico del Colegio Oficial de Bibliotecarios, Documentalistas de Cataluña, CODBC, 2006	Art. 5 Librarian-documentalists' decision-making must not be swayed by internal or external pressure, and they must perform their duties in accordance with utmost professionalism and objectivity. Art. 10 Personal data and the use of the services rendered are subject to professional secrecy. All necessary measures must be adopted to guarantee the protection and confidentiality of this information. Personal data may only be disclosed where explicitly authorised by the subject or as specified by law.

Many students working toward a degree in information and documentation have a professional profile that indisputably qualifies them for a variety of tasks in intelligence. The employment opportunities for such students in national security-related positions in intelligence and law enforcement agencies have been addressed in analyses of each service's intelligence careers[17]: from CIA librarian or record manager with the Australian intelligence service or the UK's M16, to government archive technicians and document librarians, all described in detail by Linda P. Carvell.[18]

LIS students, in turn, are among the best poised to steer their professional profiles not only toward information and documentation, but also toward intelligence analysis by taking master's or other postgraduate courses comprising "higher intelligence education" and so-called intelligence studies.[19] As noted by Stephen Marrin,[20] an academic and practitioner, all the foregoing and the present training for intelligence analysts reinforce the association between agencies and universities, two worlds doomed to mutual understanding, whose relations are not always harmonious. Indeed, the obstinate and domineering behaviour and disrespect for academic freedom and independence exhibited on occasion by the services are the object

[17] Mary Lee Kennedy, Angela Abell, "New roles for Info Pros", Information Outlook, 12: 1 (Jan. 2008). pp. 25-36.

[18] Linda P. Carvell, Career opportunities in Library and Information Science, N. York, Ferguson, 2005.

[19] Martin Rudner, "Intelligence Studies in Higher Education: Capacity-Building to Meet Societal Demand", International Journal of Intelligence and CounterIntelligence,22:1 (2009), pp. 110-130.

[20] Stephen Marrin, "Training and Educating U.S. Intelligence Analysts", International Journal of Intelligence and CounterIntelligence, 22:1 (2009), pp. 131-146. Stephen Marrin, Improving Intelligence Analysis: Bridging The Gap Between Scholarship And Practice, New York, Routledge, 2011.

of reproach in The CIA on Campus, edited by Philip Zwerling.[21]

LIS students' profiles are well matched to many of the phases, sub-phases and areas involved in intelligence generation. Archive organisation, standardised document description, application of markup languages such as XML, metadata generation, ontologies, terminology control, thesaurus design and formulation, search strategy refinement, open source information identification and updating, intelligence visualisation, application of scientometric studies and data mining are but a few of the many skills they should acquire in our classrooms. And they devote time not only to information skills obviously applicable to OSINT, but also to text filtering, indexing, summarising and analysis. The knowledge generated adopts forms and typologies not far removed from the formats used by today's intelligence bodies: reports, briefings, presentations, in-house notes and analyses of the status quo. All this training affords students a fair chance of success in intelligence agency hiring processes.

Trawl fishing: the false perception of metadata and "blind espionage"

In a recent interview on the occasion of the publication of his latest novel, Sweet Tooth, Ian McEwan was asked about the planet-wide wiretapping conducted by the United States and its partners in conjunction with other allied services at around the same time as the release of his novel. He replied that since intelligence services spy without asking why or for what purpose, the present events are not surprising, although they are fascinating (El mundo, 30 October 2013, p. 47).

OSINF is on the brink of the next great change in intelligence: full automation. Machines retrieve the information needed based on search parameters, specific equations, search term monitoring, control of terminology by means of thesaurus, and user profiles tailored to needs and requirements, selectively disseminating information meticulously formulated in the past by conventional documentalists and information management professionals. The simultaneous gathering of vast volumes of data in real time from millions of individuals the world over necessarily calls for a system which at the very least poses problems of efficiency and effectiveness: for want of the capacity for a priori discrimination and refinement, everyone's data is searched. The vast technological systems and capacity that render mass data interception feasible are naturally deployed for that purpose. The real issue lies not there, however, but in the true answer to the following question: are all those data pertinent to security and defence? If not, what is done with the data that should be discarded and deleted because they affect personal privacy? Who assesses the metadata which is of no interest to an intelligence service? How is legal storage being practised? Is everything valuable? The systems referred to here acquire information blindly, seeking not quality but quantity.

Massive data gathering can be likened to trawl fishing in which vessels' nets catch not only valuable species such as tuna, but also crab, octopus, tyres and even empty Coca-Cola cans. Data seem to be collected indiscriminately, with no appraisal or pre-analysis: data are gathered but no intelligence is acquired. Who discards the millions of data items that are unrelated to threat identification or risk confirmation directly related to national security? How and when are they discarded and what record is kept of their deletion? Here again is where information and documentation managers should apply their knowledge and skills to complex, systematic and highly technical records appraisal methodology and the "refined art of (document) destruction". And they must do so in keeping with identification, selection and evaluation protocols subject to scrutiny by highly competent legal experts, archivists and domestic security managers. For all the foregoing,

[21] Philip Zwerling (ed.), The CIA on Campus: Essays on Academic Freedom and the National Security State, Mcfarland & Co Inc., 2011.

the competence to identify, select and destroy data and documents under the supervision of document classification commissions acquires renewed importance and a new perspective in connection not only with record management, but also with personal data protection. The codes governing the conduct of archive professionals employed in intelligence agencies should play an instrumental role in the strict implementation of principles, criteria and rules for the use of data solely and exclusively relevant to securityand defence-related investigations. All other data, where acquired, must be swiftly and entirely deleted, not stored "just in case" or accumulated in vast repositories whose existence is ultimately forgotten.

Discriminatory, weighted and highly refined data retrieval is, then, not only an ethical and legal obligation in line with the right to the protection of personal information, but also a quality indicator with an impact on the efficiency and effectiveness of the outcome: not all data are usable for intelligence purposes. Not to mention the financial implications of mass data collection: why spend large amounts of public money on automatic systems that retrieve everything from everyone? Does that constitute efficient control of intelligence spending? A number of approaches to quality control in open information source collection and use have been devised in the framework of information/intelligence auditing,[22] along with others geared towards validating the quality of the final intelligence product.[23] Indiscriminate automation to gather vast quantities of raw information from which to generate new knowledge may lead to widespread organisational chaos. The result may be a blatant historic error of the same calibre as the institution of technology (SIGINT) to the detriment of HUMINT, which prompted severe disarray among intelligence services after the collapse of the Berlin Wall and the end of the confrontation with traditional or symmetrical enemies.

We are told that interception actually affects millions of data items that refer to or inter-relate with others (metadata), but not the content itself of telephone conversations: as if metadata were of lesser importance or their interception tolerable.[24] Library scientists welcome the use of this term, coined by Jack Myers in the 1960s to mean the minimum information needed to identify an information resource.[25] A data item alone does not constitute a fully comprehensible unit, but the combination of many metadata furnishes more than enough information to define and understand a higher level of information. Examples of metadata include everything from IP or DNS addresses, headings in e-mails and descriptions of FTP-accessible files to the terms extracted by indexing/search engines:

> Metadata is frequently used to locate or manage information resources by abstracting or classifying those resources or by capturing information not inherent in the resource. Typically metadata is organized into distinct categories and relies on conventions to establish the values for each category. For example, administrative metadata may include the date and source of acquisition, disposal date, and disposal method. Descriptive metadata may include information about the content and form of the materials. Preservation metadata may record activities to protect or extend the life of the resource, such as reformatting. Structural metadata may in-

[22] Susan Henczel, The Information Audit: a practical guide, Munich, Saur, 2001. Andréa Vasconcelos Carvalho, Auditoría de Inteligencia, Gijón (Spain), Trea, 2012.

[23] Giliam De Valk, Dutch Intelligence: Towards a Qualitative Framework for Analysis, Eleven International Publishing, 2005.

[24] I recommend Brewster Kahle´s latest blog post "Phone Metadata Used To Find Informants and Kill Them": http://brewster.kahle.org/2013/11/05/phone-metadata-used-to-find-informants-and-kill-them.

[25] Heather Lea Moulaison, "Emerging trends in metadata research", Proceedings of the ASIST Annual Meeting, 49: 1 (2012), pp. 1-4.

> dicate the interrelationships between discrete information resources, such as page numbers.[26]

Relying on the mass automation of information gathering and retrieval to seek answers in the metadata universe conjures up the dichotomy between big data vs big narrative so thoroughly studied by Evgeny Morozov. A huge divide separates the series of individual data items that can be regarded as indications of the future correlation of possible events from the traditional need for an in-depth rather than a merely automatic understanding of the context and varied causes underlying these data. Another of the troubling consequences of the Snowden case documents published in The Guardian and Der Spiegel is that more emphasis is being placed on data-based prevention and action than on an understanding of the context of or an explanation for the data or the circumstances in which they were generated. Big data is concerned not with understanding but only with determining when an event is going to happen based on the interrelationships between and the correlation of pieces of information, of data: metadata. Morozov, quoting Marc Andrejevic, made it quite clear: the cost of intelligence services' (and nearly all other public and private sectors') adoption of big data is the devaluation of individual understanding, embodied in our reluctance to investigate the causes of events and our tendency to leap to their consequences. Andrejevic contends that while Google can afford to be ignorant, public institutions cannot.[27]

For all the foregoing, the enormous impact of metadata surveillance on the protection of fundamental rights cannot be overlooked. The Council of Europe has already warned against the risk of automatically processing personal data.[28] European Commission Vice-President and Commissioner for Justice, Fundamental Rights and Citizenship Viviane Reding has unambiguously stated that the protection of Europeans' personal data is a nonnegotiable fundamental right.

The European Parliament has approved a proposal that clearly subjects third party transfers of European citizens' personal data to both prior authorisation from the national body regulating data protection and the service of notice upon the data subject.[29] This obviously targets companies that cooperate with intelligence services and constitutes yet another warning about the hazards of the ongoing privatisation of intelligence. But that issue lies outside the present discussion.

Conclusions

In light of their skills and knowledge, information, archive and documentation experts trained in library science and documentation departments are ideal candidates for jobs in intelligence bodies, especially

[26] Society of American Archivists, A Glossary of Archival and Records Terminology http:// www2.archivists.org/glossary/terms/m/metadata.

[27] Evgeny Morozov, "The challenge of managing great databanks", El País, 24/06/2013; http://elpais.com/elpais/2013/06/24/opinion/1372068111_079679.html Marc Andrejevic, Infoglut: How Too Much Information Is Changing the Way We Think and Know, Taylor and Francis, 2013. [paraphrased from the original Spanish text]

[28] Recommendation CM/Rec(2012) 13 <htprotection/TPD_documents/CM%20Rec%282012%293%20E%20-%20Search%20engins. pdf> of the Committee of Ministers to member states on the protection of human rights with regard to search engines; Recommendation CM/Rec(2010)13 https://wcd.coe.int/ ViewDoc.jsp?id=1710949&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB 021&BackColorLogged=F5D383 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling (23 November 2010).

[29] Gloria González Fuster, "Security and the future of personal data protection in the European Union", Security and Human Rights, vol. 23, n. 4 (2013), pp. 33 -342.

although not solely in two well-defined areas: open source information gathering and records management/ archival organisation. Moreover, automated information gathering and retrieval is going to become so widespread and remote from human intervention that the expression "blind data collection" will ultimately prioritise vast amounts of data over the quality of refined data and pre-analysis. That, in turn, will induce system delays and the cloud storage of ever vaster volumes of wholly worthless raw information. However, not all the open information on the internet can be ethically and morally reused by third parties. The ethical implications of open information have been insufficiently analysed and studied.

Public authorities have quite obviously intercepted and continue to intercept communications, a practice that need not be traced back to Kircher's acoustic devices. The issue to be addressed is the definition and scope of the legal curbs that effectively guarantee and protect fundamental rights, as well as the ethical curbs in place, that are applicable to counter the widespread, indiscriminate and wholly uncontrolled monitoring of millions of data items. In the face of endless and growing automation and the inevitable risks stemming from personal and private data management, information and documentation professionals' ethical commitment should be a curriculum requisite reinforced in classrooms. Such training would be another tool for thwarting behaviour and attitudes that violate fundamental rights in the realm of privacy and personal data.

Last but not least: according to their solid training in ethics and respect for fundamental rights, information and documentation professionals must act in keeping with the law. Consequently, if a country has laws on official secrets and rules governing data protection and safeguards for secrets, information professionals (especially if they are public servants) must abide by those provisions in the name of the law, even where they are clearly improvable or even obsolete. The problem arises when those provisions clash with the individual and social rights and freedoms that inspire and form part of a nation's fundamental laws or international declarations and conventions. The solution to this dilemma cannot be left solely and exclusively to each public official's own conscience, for that would make institutions' operation and future dependent upon each individual.

That is the reason why internal and external supervisory and control mechanisms and even conscientious objection must therefore be strengthened to settle discrepancies or overcome the reluctance to comply with the rules that are deemed to clash with the universal principles on which democratic systems rest. Further to the profession's codes of ethics and declarations on corruption, transparency, good governance and access to information, such as those put forward by the IFLA in 2008, information professionals should not commit illegal acts in the name of ethical principles, but should actively work to draft, amend, propose in-depth updates and expose limitations or governmental mala praxis that contravenes those fundamental rights and freedoms, within the existing legal framework.

This article was first published with Brill | Nijhoff publishers, and was featured on the Security and Human Rights Monitor (SHRM) website.

Security and Human Rights (formerly Helsinki Monitor) is a journal devoted to issues inspired by the work and principles of the Organization for Security and Cooperation in Europe (OSCE). It looks at the challenge of building security through cooperation across the northern hemisphere, from Vancouver to Vladivostok, as well as how this experience can be applied to other parts of the world. It aims to stimulate thinking on the question of protecting and promoting human rights in a world faced with serious threats to security.

Netherlands Helsinki Committee
Het Nutshuis
Riviervismarkt 4
2513 AM The Hague
The Netherlands

www.nhc.nl