JICLT
Journal of International Commercial Law and Technology
Vol.9, No.3 (2014)

Privacy Risk Area Assessment Tool for Audio Monitoring – from legal complexity to practical applications

Sébastien Ziegler
&
Papa Moustapha Kémo Sonko

Mandat International
3 chemin Champ-Baron
1209 Geneva, Switzerland
www.mandint.org
sziegler@mandint.org
&
EAR-IT European Research project
www.ear-it.eu

Abstract: The Privacy Risk Area Assessment Tool (PRAAT) for audio monitoring has been developed in the frame of EAR-IT, a European research project exploring the potential of audio monitoring for smart buildings and smart cities. The project addresses several privacy related issues in different countries and contexts, including outdoor and indoor audio monitoring. By involving real end-users in different legal environments, the project has to be very careful in respecting the privacy rights and has to make sure that its experiments are compliant with the a complex web of international, European and national obligations. Based on a detailed legal analysis, the authors have elaborated a Privacy Risk Area Assessment Tool (PRAAT) for audio monitoring. It has been designed to be user-friendly for users with limited legal background, such as researchers, public administrations and other interested stake holders in evaluating the level of legal risk bound to any project of audio monitoring deployment.

I. Introduction

The EAR-IT is a 3- year FP7 European research project on audio monitoring through the Internet of Things. It explores the potential of audio monitoring with Non Line-of-Sight (NLOS) and multipurpose sensing. It explores such applications in two test beds with real end-users in Spain and Switzerland, with indoor and outdoor experiments. However, the developed technology and research outcomes should be relevant for any European country. Audio monitoring is implicitly interacting with privacy rights that must be seriously addressed and considered in the frame of the project. In this context, the present article presents the results of a legal analysis of privacy risks related to audio monitoring as well as a practical and user friendly tool intending to reduce the risks of breaching privacy rights obligations when deploying audio monitoring. The outcomes of the project will be shared with the research community and used by other projects, such as IoT6 1 addressing the potential of IPv6 for the future Internet of Things.

1.1 Audio monitoring and Privacy

Audio monitoring can contribute to turn cities and buildings into smarter environments. It can help saving energy, protecting people and improving the end-users comfort. However, it can impact privacy rights in different ways. According to the technology used and its level of granularity, an audio monitoring system can generate and collect personal data, including private communications.

Privacy is a complex and evolving concept. The perception of privacy may vary from one society to another, from one period of time to another, and from one individual to another. Moreover, several

[1] IoT6 European project: www.iot6.eu

researches have highlighted the multidimensional nature of privacy concerns. For instance, Hong and Thong refers to six key dimensions of Internet Privacy Concerns[2], including data collection[3], secondary usage[4], errors, improper access[5], losing control on one's own data and lack of awareness. Allan Calder in a recent study highlights the risk related cyber-security and Cyber resilience. [6] Cultural background and demographic dimensions (age, gender, income, education, etc.) influence the privacy perception[7]. Researchers like Röcker have demonstrated clear differences in privacy perception between Americans and Germans which could be related to cultural and historical specificities[8].

Privacy has intrinsically a certain level of ambivalence: It is simultaneously a universal concern combined with divergent understandings, which may vary from one country to another, as well as from a domain of activity to another. This duality is reflected by a rather large number of international and regional conventions protecting privacy as well a certain level of heterogeneity among the national laws. In the frame of our research, we decided to adopt an extensive definition of privacy, encompassing:

- Personal data protection;
- Private communication and conversations;
- Private spaces, including homes and cars;
- Protecting both physical and moral persons (human beings and private companies);
- Privacy breach by public and/or private entities.

We had to address privacy in both indoor and outdoor environment, including public spaces by considering that a private conversation between two people in a public space is still subject to protection.

For the purposes of this paper, it is important to differentiate the context of audio monitoring between private and public spaces. Private space is perceived by the end-users as the privacy area by excellence. It is in principle under the control of their inhabitants. The main identified specific risks would be hidden monitoring (all or part of the inhabitants ignore the existence of the monitoring) and the lack of awareness or understanding by the inhabitants. The risk that an audio-monitoring systems is deployed in a private environment with the consent of the private space, but could constitute a privacy breach for visiting third parties, such as guest or employees. Work spaces are private space with third parties involved. In some legislation, audio- monitoring is prohibited or requires an obligation to inform the employees about the monitoring system and its location. A risk remains for visitors who may not be aware of on-going audio monitoring. Outdoor and indoor public spaces are accessible to everybody. There are direct risks related to accessing private conversations and collecting personal data without informed consent.

2. Main privacy risks related to audio monitoring

In order to identify the main privacy-related risks with audio monitoring, EAR-IT project has requested the support of experts on this topic and has launched a public survey with 1'000 European citizens who have been questioned on their perception of privacy risks and audio monitoring. By combining both inputs from the public and the experts, we have synthetized a rather exhaustive list of related risks including:

---

[2] Hong, Weiyin and Thong, James Y.L.. 2013. "Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies," MIS Quarterly, (37: 1) pp.275-298.

[3] Malhotra, N.K. et al. 2004. Internet Users' Information Privacy Concerns (IUIPC). Info. Sys. Research. 15, 4, 336–355.

[4] Junglas, I., Johnson, N., & Spitzmüller, C. 2008. Personality Traits and Concern for Privacy: an Empirical Study in the Context of Location-Based Services. [Article]. European Journal of Information Systems, 17(4), 387-402.

[5] Smith, J., Dinev, T., Xu, H. "Information Privacy Research: An Interdisciplinary Review," MIS Quarterly Vol. 35 No. 4 pp. 989-1015/December 2011

[6] Allan Calder "Cyber Security: a critical business issue" August 2013, "IT governance green paper"

[7] Kim Bartel Sheehan « An investigation of gender differences in on-line privacy concerns and resultant behaviors", Journal of Interactive Marketing, article first published online: 28 February 2000.

[8] C. Röcker. Information privacy in smart office environments: a cross-cultural study analyzing the willingness of users to share context information-In Proc. ICCSA, 2010.

- *Accessing private communications and discussions*.
- *Personal identification and geo-localization*, which enters into the personal data protection scheme and triggers a set of European obligations.
- *Voice and personal data transmission*, with the risk to transfer personal data without control and/or through unsafe/vulnerable channels of communication.
- *Data storage*. By keeping record of personal conversation or information, we are extending the privacy interaction to the past. It also raises the issue of data ownership and informed consent.
- *Third parties access to personal* data, which can include sensitive information on health, intimate life and/or sexual orientation.
- *Personal data dissemination*. A user may agree that its municipality collects personal data, but may consider quite illegitimate if such information would be made publicly accessible to third parties. Moreover, it creates a risk of irreversibility: as long as the information is located in a specific entity, it is still possible for the concerned person to request a rectification and or to erase its personal data. Once the data is disseminated in the wild, the person loses its right to control, rectify and erase his personal data.
- *Extended information risk*. Audio monitoring can provide richer information than expected, in particular if such data can be combined with other data to provide extended and richer information on people. With this view, anonymized audio data could be linked to individuals by crossing them with other data (such as video surveillance).
- *Legal risk* (compliance with international, EC & national norms) enhanced by the complexity of the norms related to privacy rights and data protection.
- *Disagreement on data use*. A large part of the respondents to the survey seemed to agree with audio monitoring as long as a clear and legitimate purpose is provided. However, they disagree having their data used for other purposes.
- *Societal and media rejection*. Beyond the legal dimension of privacy obligation, there is a risk of subjective rejection of the audio monitoring. It is conceivable that an audio monitoring infrastructure be deployed legally in a public space and face a strong rejection by the public opinion and the media.

3. Legal Environment

The privacy protection is addressed by several international, regional and national and obligations. Taken together, these norms constitute a complex legal framework.

3.1 International legal framework

Privacy enjoys legal protection from several core international treaties and conventions, including the Universal Declaration of Human Rights of 1948 (UDHR)[9] and the International Covenant on Civil and Political Rights (CCPR)[10]. Several treaties related to specific groups of persons and specific domains contain similar binding commitments in their core text, such as the Convention of the rights of the Child[11], the International Convention on the Protection of the Rights of All Migrant Workers and Members of their Families[12], and the Convention on the Rights of persons with disabilities[13]. We should also mention the International Telecommunication Convention as a relevant international framework with a focus on communications. All these basics texts are quite consistent and set the basis for a fundamental principle: The obligation for members States to protect individuals against arbitrary or unlawful interferences or attacks with their privacy[14] and the obligation to protect secrecy in international correspondence and communications[15]. These obligations are formally and materially binding the ratifying parties.

---

[9] The Universal Declaration of Human Rights, http://www.ohchr.org/EN/UDHR/Documents
[10] International Covenant on Civil and Political Rights, New York, 16 December 1966 at *http://treaties.un.org/pages/CTCTreaties;*
[11] Convention on the Rights of the Child, http://www.ohchr.org,
[12] Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, http://www2.ohchr.org/english/bodies
[13] http://www.un.org/disabilities/convention
[14] Article12 and Article 17 of the UDHR and International CCPR respectively
[15] International Telecommunication Convention Concluded at Nairobi, 1982

In parallel, the privacy protection framework is evolving with emerging soft law, such as the Organisation for Economic Co-operation and Development (OECD)' guidelines on the protection of privacy and trans border flows of personal data[16] are for example, which has substantially influenced many personal data Acts in the World.

3.2 Regional legal framework

The regional level has enabled the emergence of more specific obligations. At the European level, privacy obligations are mainly shaped by the Council of Europe and the European Union. The Council of Europe has led the development of the European corpus of Human rights with explicit references to privacy rights. It includes the Convention for the Protection of Human Rights and Fundamental Freedoms, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data "Convention 108", the Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the application of Biology and Medicine, and the Convention on Cybercrime. These conventions converge on the need to protect personal data requiring a protection at every step, from collection to storage and dissemination.

The European Union norms can be differentiated in two categories of norms: primary and secondary norms. At the primary norms level, the right to protection of personal data is established by Article 8 of the Charter and Article 16 of the Treaty on the Functioning of the European Union (TFEU) and in Article 8 of the European Convention on Human Rights **(**ECHR). The European Union has adopted two major treaties containing legal obligations related to privacy: the Charter of Fundamental Rights of the European Union adopted in 2000, and the Treaty establishing a Constitution for Europe adopted in 2004. It is completed by a set of conventions, including the Convention on the establishment of a European Police Office (Europol Convention), the Convention implementing the Schengen Agreement of 14 June 1985, and the Convention on the use of information technology for customs purposes (CIS).

The secondary norms level includes regulations and directives such as those applying to data processed by automated means (e.g. a computer database of customers) and data contained in or intended to be part of non-automated filing systems (traditional paper files). The reference Act at the European level is the European Parliament and Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. This Directive "*sets strict limits on the collection and use of personal data and demands that each Member State set up an independent national body responsible for the protection of these data.*"[17] It is completed by a set of specific directives mainly on data access and electronic communications in order to ensure that citizens and users can trust their authorities as well as "*the services and technologies they use for communicating electronically*"[18]. Other norms have an impact on privacy rights, including Council Regulations, Communications, Recommendations (such as the Recommendation 2006/952/EC for the protection of minors and human dignity in audio-visual and information services), and opinions given by the Working Party of the data protection framework. Those various texts focus mainly on the protection of personal data with some key principles:

- The right to be informed;
- The informed consent principle, ensuring that individuals are aware and give their agreement to personal data collection;
- The lawfulness and fairness principles;
- The need and proportionality principle: personal data should not be collected more than needed, neither stored for a longer period than needed;
- The right of integrity and security of data;
- The right to access and to rectify collected data;
- The strict protection of the rights of individuals in case of cross-border data transfer.

[16] http://www.oecd.org/internet/ieconomy/oecd
[17] http://europa.eu/legislation_summaries
[18] http://europa.eu/legislation

The APEC privacy framework has some similarities with EU privacy framework. Both are aligned with the 1970 fair information practice principles (FIPPs)[19] and OECD guidelines. They share the same concerns about privacy risks. However, they differ markedly on the objectives of privacy protection. The APEC framework is focused on "harm prevent notion" a "harm resulting from wrongful collection and misuse of personal information", while the European data Act[20] protect individual privacy as a fundamental right, and regulate the collection, use, disclosure and other processing of personal data accordingly. The APEC framework is built on some key principles:

- The "preventing harm" principle, requiring mainly internal actions to avoid misuse of personal information and consequent harm to individuals;
- The notice principle, ensuring that individuals are able to know what information is collected about them and for what purpose it is to be used;
- The data collection and use should be limited to the purpose for which it is collected;
- The lawfulness and fairness principles;
- The choice principle allowing individuals have their say in the collection, use, transfer and disclosure of their personal information.
- The principle of integrity of personal data

Both regional frameworks share similarities with some differences. They also recognize the possibility to override the above mentioned principles when public interest requires it.

3.3 National legal framework

At the national level, we are facing a heterogeneous set of obligations, varying from one country to another. This situation increases the risks of privacy breaches for organisations operating in more than one country. The diversity also impacts the way international and European norms are translated internally. A recent Article of NeoLex Avocats on Europe said that: "differences of data protection within the 27 member states would cost 2.3 billion euros per year to companies that are doing the splits between their specific policies for handling personal data and heterogeneity of different national laws".[21] Differences may be quite large. To mention a simple example, countries like Switzerland are extending privacy law to legal persons, while other countries, like France, are limiting it to natural persons. This heterogeneity may be difficult to harmonize due to diverse historical and cultural backgrounds, which impact the way privacy is perceived and the role the State should play in this context.

3.4 On-going evolution

The privacy rules and obligations are evolving to cope with new technologies and a changing society, where many use the Internet to communicate and store personal data in the cloud, and where the majority of the population can be physically tracked via their mobile phones. A society which simultaneously needs to protect privacy rights of its citizens and addresses issues such as terrorism and pornography. There is an inherent and on-going negotiation between the fundamental individual rights and freedoms, and the societal interests.

At the international level, European States and their counterparts in international institutions are getting involved in numerous programmes for helping to find solutions to the issues arising from the use and misuse of the Internet, of particular concern to everyday users (e.g.; Digital Agenda for Europe (the Europe 2020), Internet Governance Forum, UNESCO Code of conduct for the Information Society October 2011, Council for Europe "12 principles of Internet Governance" from the Internet Governance Forum in Lithuania 2010).

At the European level, European Commission has taken lead with its proposal to update the 1995 Directive on the protection of personal data. The proposal remains rooted in the previous Directive's spirit but ensures a higher level of protection for the users protection, particularly online privacy rights. If it is adopted it will increase harmonisation of data protection rules applicable across the EU and also

[19] http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide
[20] Directive 95/46/EC, http://eur-lex.europa.eu
[21] http://www.neolex.fr/author/neolex-avocats/ NeoLex Avocats « European Data Protection Day » – Berlin les 7 and 8 may, 2012

facilitate and alleviate the proceedings and costs upon organisation with the principle of single home country data protection authority "One stop shop".

At the American level, the administration has urged and supports the necessity of adopting the new Consumer Privacy Bill of Rights. Federal agencies are also devoted in privacy protection by producing guidance on data privacy. The Department of Health and Human Services (HHS)[22], for example, has issued guidance that enforces HIPAA Breach Notification Rule which imposes an obligation on data processors to provide notification about breaches of unsecured protected health information. Furthermore, responsible industries are stepping forward in terms of protecting user' privacy by adopting self-regulations[23] strategies. Numerous efforts at self-regulation have emerged.

3.5 Inherent complexity

As illustrated, the privacy rights are shaped by a superposition of international, regional and national norms. The resulting normative framework is highly complex. Moreover, the notion of privacy itself embeds a certain level of complexity. For instance, the European Directive on personal data protection considers any data that can be linked by "reasonable means" to a person, as personal data. Let's consider the deployment, in a smart city, of an audio monitoring system able to collect ambient sound, including human conversations. Such deployment could be considered as non-relevant from the perspective of the European Directive on personal data protection, as long as the collected data cannot be linked by reasonable means to individuals. The obligations would change substantially if a few weeks later, a video surveillance system is deployed nearby. It would then be reasonably possible to compare the two sources of information in order to link a recorded conversation to a person. As a consequence, the audio monitoring system should comply with a whole new set of obligations.

4. Synthesis of legal risks and obligations on privacy to be respected by EAR-IT

Based on the legal framework we have identified a number of aspects that needs to be handled in the frame of EAR-IT project. Privacy is clearly embedded in Human rights standards. It is hence important to consider the protection of basic human rights and the respect for private and family life, including private conversations in the frame of the present research project. EAR-IT will have to respect to align with principles such as:

- **Transparency**: data processing is governed by principles of subject's consent, validity, integrity, precision, reliability, and timeliness.
- **Legitimate purpose**: data processing should be compatible with the intended purposes.
- **Proportionality**: data should be processed and collected within specified framework and limited to what it is necessary to achieve in relation to the

We can distinguish privacy-related obligations in two categories: Obligations related to personal data and obligations related to other aspects of privacy, independently from the identification of the person:

4.1 Main obligations related to personal data

- Personal data must be processed fairly and lawfully;
- Personal data must be collected for specified, explicit and legitimate purposes and must not be further processed in a way incompatible with those purposes;
- Personal data collection should be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
- The data should be accurate and, where necessary, kept up to date;

[22] http://www.hhs.gov/ocr/privacy/index.html
[23] Eli M. Noam "*Privacy and Self-Regulation: Markets for Electronic Privacy*"

- The storage of data which permits identification of data subjects should not be longer than what is necessary for the purposes for which the data were collected;
- In principle, the personal data can only be processed if the data subject has given his/her permission and the data subject have the right to access their data and to object to the processing of their data. When it comes to surveillance of communication the European Commission stresses the importance that listening, tapping, storing and other kinds of interception or surveillance is prohibited without the consent of the user;
- Data processing must be transparent to the data subjects;
- In case of the processing of sensitive personal data or personality profiles, the law puts an obligation on the owner of the respective data collection to explicitly inform the data subjects on certain aspects of the data processing;
- The transfer of personal data to countries with a weaker level of data protection is only possible in a limited number of exceptional situations, most importantly: (1) the consent of the data subjects in the specific case (2) a data transfer agreement, approved by DPAs or using the Standard Clauses issued by the European Commission ;(3) in case of a group internal transfer, group internal data protection guidelines;
- The data subjects have a right to information regarding their data.
- Individuals have the "right to be forgotten" by having their data removed upon request. This new principle shall be enshrined if the Commission's proposal on data protection is adopted. [24]

4.2 Main obligations related to other aspects of privacy

- The Processor must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure and destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information may be used.
- Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.
- Everyone has the right to respect for his private and family life, his home and his correspondence[25].
- There shall be no interference by the public authority with the exercise of this right except such as is in accordance with the law, pursued with a legitimate aim and if it is necessary in a democratic society.
- Nobody can disclose personal data obtained from a data user without the data user's consent for malicious purposes, namely: (i) with an intent for gain, or to cause loss to the data subject; or (ii) where the disclosure results in psychological harm to the data subject.

5. Privacy Risk Area Assessment Tool

As previously demonstrated, the interaction between audio monitoring and privacy is complex. The privacy related obligations result from several parameters:

- Various sets of legal obligations at the international, regional and national levels,- which may vary from one country to another;
- Different contexts: indoor, outdoor, public, private, etc.
- Different forms of audio monitoring: granularity, recording, etc.

[24] http://www.telegraph.co.uk/technology/internet/8388033/Online-right-to-be-forgotten-confirmed-by-EU.html
[25] Article 8 of the ECHR, *and Leander v. Sweden*25, 26.03.1987; Kopp v. Switzerland, 25.03.1998; Amann v. Switzerland25, 16.02.2000

In order to tackle this complexity and to ease the work of researchers, we have identified and defined a few concepts and a practical tool in order to enable an easier evaluation of the risks related to audio monitoring deployment.

We define the concept of "Privacy Risk Area" as an area in which the risk to breach someone's privacy rights is high. By opposition, a "Privacy Safe Area" is an area in which the risk to breach someone's privacy rights is very low. A grey zone area is implicitly emerging between those two previous notions, where the level or risk to breach someone's privacy rights is not clearly identified. (*See figure 1*)

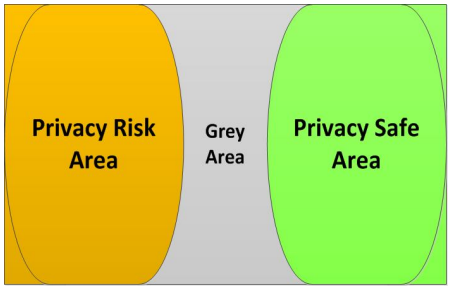

Figure 1. Privacy Risk Area (PRA) and Privacy Safe Area (PSA)

Based on those concepts, we have designed a Privacy Risk Area Assessment Tool (PRAAT). It is intended to provide a user friendly tool which would enable any researcher or public administration without legal background to estimate if a planned audio monitoring deployment is rather compliant with privacy obligations (in a Privacy Safe Area) or likely to breach some privacy rights (in a Privacy Risk Area). The proposed tool does not pretend to provide an absolute answer, but a highly accurate estimation of the privacy compliance. The Privacy Risk Area Assessment Tool (PRAAT) is a multi-criteria assessment tool based on a two steps analysis.

A - PRA Preliminary check

In a first step, we invite the user to check the following criteria:

- the system is unable to capture conversations;
- the system is unable to differentiate and recognize different speakers;
- the speakers cannot be identified by reasonable means.

If the user intended deployment complies with all the criteria, it should be in a rather Privacy Safe Area and we consider that he can stop his analysis there. If one or several of the above criteria is answered by no, the deployment will most likely trigger obligations related to personal data protection. Hence, a second set of criteria is presented to the user, in order to assess if the experiment remains in a privacy safe area.

B - PRA Complementary check

For the complementary check, we invite the user to check the following criteria are respected:

- the persons whose voice could be recorded are clearly informed (directly or through signal posting);
- the personal data and audio streams are not unnecessarily stored or recorded (any record should have a good justification and be limited in time);
- the data/audio are not accessible to third parties;
- the data granularity is limited to what is needed;
- the data transmission is limited to what is needed and in case of voice of personal data transmission beyond the premises of the audio collection, it is secured (encryption and authentication);
- the personal data and audio streams are not transferred abroad;
- In case of public areas monitoring:
- The competent authority has given a prior written agreement.
- The monitoring pursues public interests: environment protection, security, education, etc.

If a planned experiment matches all those criteria, it is considered to be in a Privacy Safe Area. If not, it has a high probability to be either in a Privacy Risk Area or in a grey area.

C - Iterative process

The PRAAT methodology enables the user to focus on the key factors of risk. In case of an unsuccessful result, the PRAAT methodology preconizes an iterative process. The user is invited to examine the key factors having caused a negative result and consider some adaptation to the deployment plan in order to mitigate those risks. Then the PRAAT should be then applied again to the adapted deployment plan. If despite the iterative process (*see Figure 2*) the result remains negative, a deeper analysis and consultation with the competent authorities is required.

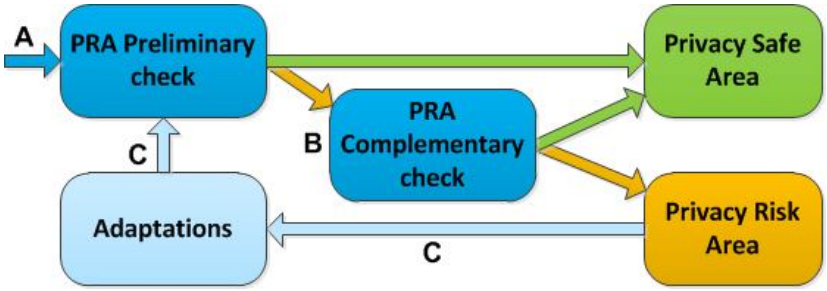

Figure 2. PRAAT iterative process scheme

6.Application to Smart Santanders and Hobnet test beds

The PRAAT methodology has been applied to the two main audio monitoring test beds of EAR-IT research project: Smart Santander and Hobnet.

The City of Santander in Spain is a pioneering European smart city associated to several international research projects, including Smart Santander. EAR-IT is deploying several audio sensors in this city to identify and locate audio events such as sirens of emergency vehicles.

The Hobnet test bed in Geneva Switzerland has been developed by Mandat International as an indoor test bed with all kinds of sensors and actuators for smart buildings. EAR-IT will deploy audio sensors to identify the presence of users and enable them to experiment richer interactions with their work environment. The targeted applications include improved energy efficiency, security and comfort. Other applications such as accessibility for people with disabilities will be considered too.

The PRAAT methodology has been applied to both test beds. In both cases, the PRAAT has enabled the identification of risk factors. Measures have been applied to mitigate the identified risk and a second iteration of the PRAAT has enabled to validate the deployment plan, by ending up in a privacy safe area for both test beds. The first results of the PRAAT are positive and have enabled to adapt the EAR-IT deployment plan to respect privacy rights and obligations. This methodology will be further tested and fine-tuned in the frame of the EAR-IT experiments.

7. Conclusion and next steps

Audio monitoring is promising technology with potential applications to smart cities and smart buildings, in areas such as energy efficiency, security and comfort. However, audio monitoring may easily breach privacy rights with several risk areas. Hence a major importance should be given to privacy issues within organisations that collect, store, use and disclose personal data. Organisations have the burden of demonstrating that two requirements are met when processing personal data:

- The compliance with numerous privacy laws in jurisdictions (national, regional and international) where the organizations do its activities and,

- The Compliance with data subject' expectations for handling their personal information.

The complex legal framework of privacy makes very difficult for researchers, public administrations and other stakeholders to make sure that such deployment is compliant with privacy rights. The PRAAT methodology provides a pragmatic and efficient way to assess the compliance of an audio monitoring deployment plan with privacy rights. The methodology will be further tested and fine-tuned by Mandat International in the frame of the EAR-IT European research project.

At a meta level, EAR-IT intends to use and fine tune the PRAAT approach to support the transition towards privacy friendly solutions, based on privacy by design and able to pave the way to a better user acceptance of audio monitoring. In this context, the authors are welcoming cooperation with other research teams to extend, fine tune and validate the proposed model.

.* * * * *

Cite as: Ziegler, Sebastian and Sonko, Papa Moustapha Kém. Privacy Risk Area Assessment Tool for Audio Monitoring – from legal complexity to practical applications, *Journal of International Commercial Law and Technology.* Vol. 9 No.3 (July, 2014)