

Legal and Ethical Challenges in Recording Air Traffic Control Speech

Mickaël Rigault^{*1}, Claudia Cevenini^{*2}, Khalid Choukri¹, Martin Kocour³, Karel Veselý³, Jan Černocký³, Igor Szoke⁴, Petr Motlíček⁵, Juan Zuluaga-Gomez⁵, Alexander Blatt⁶, Dietrich Klakow⁶, Allan Tart⁷, Pavel Kolčárek⁸,

European Language Resources Association¹, Romagna Tech², Brno University of Technology³, Replaywell⁴, Idiap Research Institute⁵, Saarland University⁶, OpenSky Network⁷, Honeywell⁸.

9 rue des Cordelières, 75013 Paris, France¹ ; Romagna Tech, Corso Giuseppe Garibaldi 49, Forlì 47121, Italy² ; Brno University of Technology, 61200 Brno, Czech Republic³ ; Replaywell, 61200 Brno, Czech Republic⁴; Idiap, 1920 Martigny, Switzerland⁵; Saarland University, 66123 Saarbrücken, Germany⁶; OpenSky Network, 3400 Burgdorf Switzerland⁷; Honeywell, 62700 Brno, Czech Republic⁸

mickael@elda.org, claudia.cevenini@studiocevenini.it (corresponding authors), choukri@elda.org, ikocour@fit.vutbr.cz, iveselyk@fit.vutbr.cz, szoke@replaywell.com, motlicek@idiap.ch, juan-pablo.zuluaga@idiap.ch, tt@lsv.uni-saarland.de, dklakow@lsv.uni-saarland.de, tart@opensky-network.org, l.kolcarek@honeywell.com, cernocky@fit.vut.cz.

Abstract

In this paper the authors discuss the various legal and ethical issues faced during the ATCO2 (Automatic Transcription and Collection of Air Traffic Control) project. This project has received funding from the Clean Sky 2 Joint Undertaking (JU) under grant agreement No 864702 and support from the European Union's Horizon 2020 programme.

This project is aimed at developing tools to automatically collect and transcribe air traffic conversations, especially conversations between pilots and air controls towers.

The authors will develop issues related to intellectual property, public data, privacy, and general ethics issues related to the collection of air-traffic control speech.

Keywords: Speech, Air Traffic Control, Intellectual Property, Public Data, GDPR, Ethics

1. Definition of Air-Traffic Control Conversations

The aim of the ATCO2 project is to develop a unique platform allowing to collect, organize and pre-process air-traffic control. According to Wikipedia¹, Air Traffic Control (ATC) is a service provided by ground-based air traffic controllers. Its purpose is to prevent collisions and organize the flow of air traffic. It is usually provided by Air Navigation Service Providers (ANSP) or Air Traffic Services Providers (ATSP) in defined sections of the airspace.

In general terms, the airspace is highly regulated by international conventions such as the Convention on International Civil Aviation² (known as the Chicago Convention) whose goal is to promote collaboration in the management of the airspace. This convention led to the inception of the International Civil Aviation Organisation, which is directed by 193 governments within the organization of the United Nations.

However, after reading the terms of this Convention and its various annexes we did not manage to find out a single regulation either allowing or disallowing the recording of Air Traffic Control Conversations.

Without specific international regulation we therefore had to turn to national legislations and more general legal concepts to try to define a legal status fitting for Air Traffic Control Conversations.

2. Air Traffic Control Conversation as IP protected material

The first hypothesis we looked at was to consider Air Traffic Control Conversations as material that may be protected by intellectual property rights.

The reason for doing so was that we could think that either ANSP or air companies may have some rights over the conversations in which their employees partake during ATC.

Therefore, the first thing we considered was the protectability of these conversations under basic concepts of Intellectual Property Protection.

2.1 Originality of Air Traffic Control conversation

When considering whether Air Traffic Control Conversations recordings can be defined as original material capable of being protected under intellectual property principles, we need to figure out whether they meet the threshold of originality which is essential in major legal systems to grant creations legal protection

2.2 Originality under US Law

Under Section 102(a) of the US Copyright Act, copyright protection is granted to a list of original works of authorship including in sound recordings.

The United States Supreme Court decided in its landmark case, *Feist Publications, Inc v. Rural Telephone Service*

¹ https://en.wikipedia.org/wiki/Air_traffic_control

² https://www.icao.int/publications/Documents/7300_cons.pdf 79

*Co., Inc.*³, that copying of telephone listing without a license did not constitute a copyright infringement.

The Court held that copyright protection necessitates “*independent creation plus a modicum of creativity*” and that facts in themselves are not original and thus are not copyrightable. The Court also decided that compilation of facts however may be original since the author may choose the facts to include, and the arrangement of these facts to allow readers to use those facts.

2.2.1 Originality under EU Law

In the European Union, the Courts have been at the forefront of the definition of the originality criteria.

In two cases the European Court of Justice provided for further details to the definition of originality necessary to pass the threshold of copyright protection.

In *Infopaq International A/S v. Danske Dagblades Forening*⁴, a media monitoring company provided summaries of articles published in Danish Newspaper to its customers thanks to a “data capture process” without authorisation. In its judgment, the court held that copyright apply only in relation to a subject matter which is original in the sense that it is the “author’s own intellectual creation” (Rec. 37). The author’s creativity can express itself through the choice, sequence, and combination of words.

In *Football Association Premier League et al v QC Leisure et al. and Karen Murphy v Media Protection Services Ltd.*⁵, certain public places located in the United Kingdom used foreign decoder devices and cards to allow them to receive broadcasts of the English Football Premier League from other EU countries. The Football Association Premier League viewed these activities as harmful for their activities as it undermined the territorial exclusivity of broadcasting rights they grant to a certain territory.

In this context, the Court ruled that football matches were not classifiable as copyright protected works under the Copyright Directive⁶, since the rules to the game leave no room for creative freedom (Rec. 98).

2.2.2 Characteristics of ATC Speech

During the ATCO2 project, we observed that ATC speech bore certain characteristics that led us to think that these conversations do not meet the threshold of originality required to be considered as such as protected by Intellectual Property.

The first thing is that air-traffic conversations are broadcast in the airspace, which is part of the public domain. Indeed, it is fairly known that there are

community of enthusiasts listening or recording to ATC speech.

Moreover, the conversations held in that context must respect a strict phraseology to ensure proper communication between the parties, for an example refer to the guide published by Eurocontrol, the association of European ANSPs⁷.

Finally, the conversation must be made in a purely utilitarian fashion and do not require the controllers or the pilots to perform any sort of choice on the words they use since they must communicate exact information to each other.

Therefore, we can assume that ATC Speech as such cannot be considered Intellectual property material that can be appropriated by either the companies, the ANSPs or the pilots.

2.3 ATC Databases

Even if we can exclude ATC speech as protectable in essence, we thought that the collection of ATC speech in databases may be protected.

Both in US and European Law, collections of works are protected respectively by Section 103 of the Copyright Act and by the Directive on the legal protection of databases⁸.

In both legislation databases are defined as collections of independent works or information. In this regard it is the effort made by the producer to compile the database to arrange the data and do not extend to the data itself.

Therefore, we thought that ANSPs may have in their possession databases of recordings of ATC speech. However, after contacting some private ANSPs it appeared that they were not willing to license the rights to use those databases for our purposes.

As example, as detailed in Section 3.2. we tried to contact the National Air Traffic Service which operates in the United Kingdom. However, during our e-mail exchanges with them to try to obtain their records of air-traffic conversations, they declared that they only made available these records upon receipt of a Court order. This would hint that they would have such databases but we could not obtain any detail regarding the extent of these databases.

That is why we tried to figure out a way to obtain the data without asking licenses to ANSPs, leading to our next hypothesis.

3. ATC as public data

Our final hypothesis was to consider ATC speech as public data. This hypothesis rests in the fact that in most cases Air Traffic is considered as a public service which is performed by service providers providing this service under different legal forms.

³ *Feist Publications, Inc v. Rural Telephone Service Co., Inc.*, 499 U.S. 340

⁴ *Infopaq International A/S v. Danske Dagblades Forening* C-5/08

⁵ *Football Association Premier League et al v QC Leisure et al. and Karen Murphy v Media Protection Services Ltd.* C-403/08

⁶ Directive (EU) 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society

⁷https://www.easa.europa.eu/sites/default/files/dfu/EGAST_Radiotelephony-guide-for-VFR-pilots.pdf

⁸⁰ Directive 96/9/EC on the legal protection of databases

3.1 Public Sector Information Directive

The European Union provides for a harmonized framework for the access and reuse of Public Sector Information (PSI)⁹. This Directive provides for rules facilitating the collection and re-use of documents produced by public sector actors.

This Directive provides that documents produced by public authorities, public enterprises, and other public bodies can be reused by third parties for commercial or non-commercial purposes upon request.

- France

We had a look at France as one of the major countries where the collection is to take place.

Relying on the provisions of the national rules related to the reuse of public sector information we made a request to the “Direction Générale de l’Aviation Civile” (General Directorate for Civil Aviation), which is the public administration in charge of managing French airspace.

In our request we detailed the data that we wanted to obtain as well as the piece of legislation we relied upon to get the data (here Article L.311-1). In the absence of reply we made an appeal to the French “Commission d’Accès aux Documents Administratifs” (Access to Administrative Documents Commission) (CADA). In its opinion number 20205215, the Commission declared that recording controls are public documents and therefore can be communicated to applicants.

However, in its reply to the Commission the DGAC stated that there was no automatic method to differentiate between civilian and military conversations. Moreover, it was added that the conversations would allow to identify the speakers.

Therefore, it was decided that communicating those recordings would pose a threat to national security and privacy, which are valid concerns to withhold communications of public documents under section L.311-5 and L.311-6 of the “Code des Relations entre le Public et l’Administration” (Relations between the Public and the Administrations Code)

3.2 Freedom of Information Legislations

In the United States, the framework rests upon the right to be informed and has been implemented through the Freedom of Information Act¹⁰ (FOIA)

This legislation compels federal agencies to provide copies of all records produced by the agency upon request. However, the applicant makes its request in accordance with the requirements of the agency.

In the following we will go through some of the use case that we encountered during the project for specific countries.

- United States

To obtain records from the United States, we submitted a request under the FOIA to the Federal Aviation Authority (FAA).

We submitted a request for Air traffic records as is made look possible on the website¹¹. However, in our following exchanges with the FAA we found out that we had to provide for specific zones to pull the request (either via latitude and longitude or air traffic control centres.

In the follow up of our exchanges we also found out that surveillance data (radar track data) was kept for a long period of time. Nevertheless, it was indicated to us that conversations were kept only for a period of 45 days before being erased unless necessary for security reasons.

- United Kingdom and New Zealand

When we looked at the British legislation, we faced a major legal block. Indeed, the Wireless Telegraphy Act¹² provides in Section 48 that the use of devices to intercept and disclose information relative to the content of a message sent by wireless telegraphy (i.e. radio communications) constitutes a criminal offence.

We also tried to contact the National Air Traffic Service who is United Kingdom’s Air Navigation Service Providers, however it refused to make its records available in application of the provisions of the United Kingdom Freedom of Information Act, or the Re-Use of Public Sector Information Regulation which implement the PSI Directive in UK Law.

In New Zealand we also faced a similar block. The section 133A of the Radiocommunications Act prohibits to reproduce and publish the existence of the conversations held in the context of air traffic.

4. Protection of personal data

ATC voice recordings are strongly standardised and concern flight-related issues; thus, they may rarely contain the mentioning of personal data.

This, however, cannot be *a priori* excluded in absolute terms, and even in the absence of personal information, data protection related issues would need to be investigated.

4.1 Applicability of data protection laws

Personal data processing according to Reg. (EU) 2016/679 (GDPR) is a very broad concept. It refers to any action performed to pieces of information, which may – directly or indirectly – identify a person.

Even if there is the slightest chance of processing personal data, then all applicable legal requirements for ethical and legal compliance should be met.

⁹ Directive 1019/1024/EU on open data and the reuse of public sector information

¹⁰ 5. U.S. Code, §552 available at <https://www.justice.gov/sites/default/files/oip/legacy/2014/07/23/foia-final.pdf>

¹¹ https://www.faa.gov/foia/foia_coordinators/ato_service_center/s/?section=ato_request

81 ¹² <https://www.legislation.gov.uk/ukpga/2006/36/contents>

There exist some exceptions that may exempt some data processing in the field of recording air traffic conversations such as the ones detailed below:

- Household exception

ATC voice recordings are often taken by individual enthusiasts, who listen to conversations between airplanes and control towers and can share them on dedicated online platforms.

The GDPR does not apply whenever personal data are processed by a natural person during a purely personal or household activity, without a connection with a commercial or professional activity.

This could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities.

However, one thing is recording and listening privately to ATC records, a different thing is sharing the recordings with an indefinite number of persons.

In any case, regardless of the applicability of the GDPR, it should be remembered that any activity, even if carried out for purely personal and household purposes, should never cause any damage to third parties.

- Protection of threats to public security

We can also exclude the processing of personal data that is carried out by the ANPSs. We feel they can be excluded on the grounds of an exception. This exception provides that the GDPR is not applicable to processing activities linked to the prevention of threats to public security.

It is not difficult to see how the security of airspace can be closely linked to public security and that recordings of air traffic conversations are necessary to ensure the safety of passengers.

However, this may not apply to the data collected by some of the partners involved in this project therefore as a safety measure we can apply the principles of data protection.

- Use of non-personal data

Researchers could freely use anonymous, non-identifying data. Thus, adopting anonymisation techniques would be an interesting option to be explored.

We may think of solutions that would directly anonymise speech of the air traffic controllers and pilots without degrading the safety of airspace while also maintaining the confidentiality of the speakers involved.

While we did not manage to find implementations of such methods for air traffic control. We feel that any processing of air traffic control conversations imposes the compliance with the legal obligations imposed by GDPR.

4.2 General principles of data protection

When dealing with personal data, the GDPR provides for a whole set of obligations upon the controller of the data who performs the processing of the data.

There are two overarching principles that guide how the data are supposed to be handled by controllers. The first one is a principle of accountability which lets rest the responsibility of the processing activities on the controller.

The second principle is one of “privacy by design and by default”. According to this principle, controllers are obliged to think about the privacy of the users from the design of the processing and make sure that it is protected from the beginning of the project and at every step.

This in turn is turned into a set of principles that are applicable to any type of processing activities (lawfulness of processing, transparency, data minimisation, purpose limitation, storage limitation, integrity and confidentiality)

The use of pseudonymisation techniques, could be very useful in this sense as they can be regarded as a security measure. Pseudonymised data are in fact still personal data, even if only indirectly identifying.

4.3 Voiceprints and handling of biometric data

Even if recordings contained no personal data at all, they would however have to be managed with caution: voiceprints are biometric data, like a fingerprint.

Not only are they potentially identifying, but they would fall within the “special categories” of data when used to uniquely identify a person.

In this regard they are to be processed only if certain conditions are met. During the project we identified three provisions from Article 9 GDPR that could help provide a legal basis for processing.

- Explicit consent from the data subject
- Processing related to data manifestly made public by the data subject
- Processing necessary for reasons of substantial public interest

From a data protection perspective, biometric technologies, in general, are closely linked to specific physical, physiological, behavioural or even psychological characteristics of a person, and some of them might also reveal sensitive data.

As to the voice, biometrics may concern the analysis of the tone, pitch, cadence and frequency of a person’s voice, which can make it possible to determine if a certain person is who he/she declares to be, or the identity of an unknown person, if matched with data from other databases.

Biometric data may also allow for automated tracking, tracing or profiling of persons and, as such, their potential impact on the privacy and the right to data protection of individuals is high, as also observed by the EU data protection authorities.

Moreover, biometric data are irrevocable: a breach concerning biometric data threatens the further safe use of biometrics as identifier and the right to data protection of the concerned persons for which there is no possibility to mitigate the effects of the breach.

5. Conclusions and further work

Future work may include a thorough analysis of the European framework with a specific analysis of the local legislation regarding the availability of Air Traffic Control speech under open data regulations.

As well as an in-depth investigation into the exceptions granted to processing of sensitive data for reasons of public interest as well as their transcription into national legislations.

6. Acknowledgements

The ATCO2 project has received funding from the Clean Sky 2 Joint Undertaking (JU) under grant agreement No 864702. The JU receives support from the European Union's Horizon 2020 research and innovation programme and the Clean Sky 2 JU members other than the Union.