The Legal and Ethical issues Workshop @LREC2022, page 48
Marseille, 20 June 2022

Brij Mohan Lal Srivastava, PhD
Co-founder of Nijta at Inria Startup Studio, Lille

Voice Anonymization and the GDPR

Keynote Speech for the Joint Workshop on Legal and Ethical Issues in Human Language Technologies and Multilingual De-Identification of Sensitive Language Resources, LREC 2022, Marseille, 24 June 2022

Large-scale centralized storage of speech data poses severe privacy threats to the speakers. Indeed, the emergence and widespread usage of voice interfaces starting from telephone to mobile applications, and now digital assistants have enabled easier communication between the customers and the service providers. Massive speech data collection allows its users, for instance researchers, to develop tools for human convenience, like voice passwords for banking, personalized smart speakers, etc. However, centralized storage is vulnerable to cybersecurity threats which, when combined with advanced speech technologies like voice cloning, speaker recognition, and spoofing, may endow a malicious entity with the capability to re-identify speakers and breach their privacy by gaining access to their sensitive biometric characteristics, emotional states, personality attributes, pathological conditions, etc. Individuals and the members of civil society worldwide, and especially in Europe, are getting aware of this threat. With firm backing by the GDPR, several initiatives are being launched, including the publication of white papers and guidelines, to spread mass awareness and to regulate voice data so that the citizens' privacy is protected.

In this talk, I will present our startup project Nijta and its timely efforts to bolster such initiatives. Nijta proposes solutions to remove the biometric identity of speakers from speech signals, thereby rendering them useless for re-identifying the speakers who spoke them. Besides the goal of protecting the speaker's identity from malicious access, the underlying algorithm aims to do so without degrading the usefulness of speech. The output is a high-quality speech signal that is usable for publication and a variety of downstream tasks. The algorithm was subjected to a rigorous evaluation protocol which was designed by us to realistically measure voice privacy and fulfill the criteria laid down by the European Data Protection Board. This protocol led to the finding that the previous approaches do not effectively protect the privacy and thereby directly inspired the VoicePrivacy initiative which is an effort to gather individuals, industry, and the scientific community to participate in building a robust anonymization scheme. Finally, I present a methodology to remove the residual speaker identity from the anonymized speech signal using the techniques inspired by differential privacy. Such techniques provide provable analytical guarantees to the proposed anonymization algorithm and open up promising perspectives for future research.

In practice, the tools developed by Nijta are an essential component to build trust in any software ecosystem where voice data is stored, transmitted, processed, or published. They aim to help the organizations to comply with the rules mandated by civil governments and give a choice to individuals who wish to exercise their right to privacy.

Nijta