PUBLIC CONSULTATION

Guidelines 02/2021 on Virtual Voice Assistants

Comments to the EDPB

We would like to thank the EDPB for this opportunity to provide feedback on the Guidelines 02/2021 on Virtual Voice Assistants (VVAs). We believe that public consultation is an important step in producing fair and robust guidance that will protect privacy with solutions that are scalable and proportionate to the intended use cases and needs of organisations.

Anonymisation of audio data

Since 2007, Privacy Analytics has been providing data anonymisation services and software for organisations in the consumer and healthcare industries. We are particularly interested in elements of the Guidelines that address and relate to the anonymisation of audio data (sections 105, 107 and 161). Anonymisation of audio recordings is a growing field: as voice-activated technology becomes more widely used, the need for speech anonymisation techniques will grow. The Guidelines provide important guidance for applying the GDPR to VVA use, and they may also influence how voice anonymisation is handled in other contexts.

From our experience working in this space, we agree that voice anonymisation can be "specially challenging" (section 105). A voice recording can reveal personal information not only through the speech content but also through the voice attributes or biometric features of the voice itself. For example, an adversary or acquaintance could exploit or inadvertently recognise the unique aspects of a person's voice and identify them. Other voice attributes may also reveal demographic information about a person, such as sex, age or ethnic origin. Such attributes can conceivably be used in conjunction with those revealed in the speech content to identify an individual. A complete voice anonymisation strategy would need to address all these potential sources of personal information, and consider technical and organisational controls that can limit the threat landscape.

We are pleased that the Guidelines acknowledge the research being done in the field of voice anonymisation (section 105), and we are optimistic that effective voice anonymisation solutions will eventually be achievable. As the Guidelines acknowledge (footnote 37), the VoicePrivacy initiative was launched in 2020 to promote the development of privacy preservation tools for speech technology (Tomashenko et al.) and papers have already been produced in response to their 2020 Challenge (Espinoza-Cuadros et al.; Champion et al.; Dubagunta et al.). Moreover, other very recent papers on audio anonymisation show promising results. For example, Yoo et al. claim that their method successfully anonymised voice data while maintaining a high degree of speech recognition accuracy. Their method could allow VVA users to listen to their own anonymised speech, allowing them to judge for themselves whether the voice transformation is adequate. Meanwhile, Kai et al. claim to have developed a hybrid voice anonymisation approach that both reduces the *speaker* recognition rate and improves the *speech* recognition rate compared to conventional signal-processing anonymisation methods.

It is worth noting that the term "anonymisation" generally has a different meaning for voice anonymisation researchers than it may under the GDPR. The VoicePrivacy Initiative defines anonymisation as "the goal of suppressing personally identifiable attributes of the speech signal, leaving all other intact attributes." (Tomashenko et al.) According to this definition, it would seem that anonymisation is complete if a speaker's voice cannot be directly identified and does not provide any meta-information directly associated with the speaker. These requirements may be necessary but not sufficient under GDPR, since they do not address speech content that could be used to identify the speaker.

We also agree with the section 123 of the Guidelines, which suggests that human review of voice recordings be limited to strictly necessary pseudonymised data. Furthermore, to ensure that the speech content has been adequately transformed and anonymised, these voice recordings may need to be transcribed into text. Software solutions that can largely automate the process of transcribing voice recordings and subsequently transforming the text to be nonidentifying may be possible, and these too are evolving.

We wish to thank you again for this opportunity to provide our views on these important guidelines, and we hope that you have found our feedback helpful and insightful. We look forward to participating in future consultations.

Sources:

Champion, Pierre, Denis Jouvet, and Anthony Larcher. "A Study of F0 Modification for X-Vector Based Speech Pseudonymization Across Gender." arXiv preprint arXiv:2101.08478 (2021).

Dubagunta, S. Pavankumar, Rob J.J.H. van Son and Mathew Magimai.-Doss. “Adjustable Deterministic Pseudonymisation of Speech: Idiap-NKI’s submission to VoicePrivacy 2020 Challenge.” VoicePrivacy website (2021).

Espinoza-Cuadros, Fernando M., Juan M. Perero-Codosero, Javier Antón-Martín, and Luis A. Hernández-Gómez. "Speaker De-identification System using Autoencodersand Adversarial Training." arXiv preprint arXiv:2011.04696 (2020).

Kai, Hiroto, Shinnosuke Takamichi, Sayaka Shiota, and Hitoshi Kiya. "Lightweight Voice Anonymization Based on Data-Driven Optimization of Cascaded Voice Modification Modules." In 2021 IEEE Spoken Language Technology Workshop (SLT), pp. 560-566. IEEE, 2021.

Tomashenko, Natalia, Brij Mohan Lal Srivastava, Xin Wang, Emmanuel Vincent, Andreas Nautsch, Junichi Yamagishi, Nicholas Evans et al. "Introducing the VoicePrivacy initiative." arXiv preprint arXiv:2005.01387 (2020).

Yoo, In-Chul, Keonnyeong Lee, Seonggyun Leem, Hyunwoo Oh, Bonggu Ko, and Dongsuk Yook. "Speaker Anonymization for Personal Information Protection Using Voice Conversion Techniques." IEEE Access 8 (2020): 198637-198645.