Revisiting Speech Content Privacy

Revisiting Speech Content Privacy

Jennifer Williams [1], *Junichi Yamagishi* [2], *Paul-Gauthier Noé* [3], *Cassia Valentini-Botinhao* [1], *Jean-François Bonastre*[3]

[1]Centre for Speech Technology Research, University of Edinburgh, UK
[2]National Institute for Informatics, Japan
[3]Laboratoire Informatique d'Avignon (LIA), Avignon Université, France

j.williams@ed.ac.uk

Abstract

In this paper, we discuss an important aspect of speech privacy: *protecting spoken content*. New capabilities from the field of machine learning provide a unique and timely opportunity to revisit speech content protection. There are many different applications of content privacy, even though this area has been underexplored in speech technology research. This paper presents several scenarios that indicate a need for speech content privacy even as the specific techniques to achieve content privacy may necessarily vary. Our discussion includes several different types of content privacy including recoverable and non-recoverable content. Finally, we introduce evaluation strategies as well as describe some of the difficulties that may be encountered.
Index Terms: privacy, speech coding, speech recognition

1. Introduction

Speech content privacy refers to the ability to conceal or mask sensitive content information within the speech signal. Determining what would be considered sensitive information ultimately depends on the use-cases. Private content may be found within particular keywords or keyphrases such as named entities (places, dates, locations, organizations etc.), or financial and medical details. In this paper, we use the term *speech content* to mean semantically meaningful words. However, this definition could be reasonably extended to paralinguistic information including mannerisms, patterns of disfluency, or high-level perceptual features like prosody and emotion.

Traditionally, speech content privacy has been rooted in the idea that a signal-emitting device can be set up within a physical space, such as an office room, to conceal what people say during private conversations. This device emits a special type of noise to mask semantically-relevant speech sounds, like words or phonemes [1, 2, 3]. Such approaches can effectively mask speech content to the point of rendering it unintelligible to nearby eavesdroppers. However, this approach provides a blanket solution. It is heavily dependent on specific room and speaker characteristics, making it challenging for the technology to generalize to a variety of scenarios [4].

Furthermore, it may not always be desireable to mask entire conversations but instead only specific content that would be considered sensitive in nature. Perhaps the most well-known form of content privacy comes from broadcasting where a sensitive phrase is masked or replaced using a 'bleep' sound. There are downsides to using a 'bleep': it does not preserve speaker characteristics, it interrupts the listening experience, and it may be irreversible. In fact, it may be preferable to simply replace a sensitive phrase with a less-sensitive counterpart. If there were perfect text-to-speech (TTS) synthesis and perfect automatic speech recognition (ASR), we could find a sensitive phrase automatically via ASR and we could replace it with a less-sensitive phrase, while maintaining characteristics of the original speakers' voice and style. The current deep learning approaches for ASR and TTS are not ideal, but, still it is possible to produce such results with these applications[1].

Although there has been recent scientific focus on speaker-centric privacy and security [5], now there is an increasing need to expand speech privacy to ensure that *spoken content* is also protected. Solutions to speech content privacy have not yet been fully explored because new use-cases are still emerging. While more and more people adapt to voice-based technologies, two main privacy issues have become prominent. First, many people have a reasonable expectation of privacy when it comes to how their devices store, process, and transmit their voice data [6]. Second, some people modify their personal behavior due to privacy concerns, such as never using voice-enabled devices in open or public spaces [7]. Both of these issues must be addressed in order for voice technology to reach full potential.

During the past few years, there were significant advances in machine learning, especially for deep neural networks (DNNs). This has been transformational to the speech technology landscape. Because of DNNs, it is possible to train models using federated learning wherein models are adapted to specific user data without the need to transmit data away from a personal device [8]. DNNs have also enabled the development of neural vocoders that produce extremely high-quality synthetic speech [9, 10] as well as multiple different approaches to speech signal disentanglement that separates speech content from speaker identity [11, 12]. This paper explores how new forms of content privacy can be developed with different use-cases in mind and provides an opportunity to re-imagine how content privacy can be used to meet the needs of society.

2. Recent Work

There is an apparent trade-off between content-based privacy and the ability to use speech in downstream tasks. Recent work in [13] examined how privacy-transformed data affects the ability to train models for automatic speech recognition (ASR) by masking named entities in the text data during model training. In particular, they sought to adapt existing text language models to account for missing (or 'masked') words from the data. While content privacy initially reduced overall ASR system performance, they successfully developed a method to adapt text language models and regained some performance. They did not describe any methods for masking the speech audio.

The Bavarian Archive for Speech Signals (BAS) offers

[1]https://www.descript.com/

an online webservice[2] that will mask speech content using a pipeline approach. An audio file is submitted to the webservice along with a list of target words. ASR is used to obtain forced alignments of words and timestamps from the audio file. The content is masked with white noise, silence, or a bleep, and a new audio file is produced. While this pipeline approach could be useful for static databases, the required forced alignments makes this solution too computationally expensive to extend to privacy scenarios that require real-time performance.

Another aspect of content privacy is related to speech codecs and compression. A new generative DNN architecture was introduced in [14] and [15], independently, with different speech technologies in mind. The architecture is a dual-encoder vector quantized variational autoencoder (VQ-VAE) that learns to disentangle speech content and speaker identity information in the speech signal while simultaneously creating a discrete and compressed representation of the speech. In [14] the goal was to use VQ-VAE to compress the speech signal and enhance it by removing unwanted noise. They measured compression rate as bits/sec as well as human judgements of the enhanced speech naturalness. In [15], they took advantage of the discrete representations to *mask the content* of targeted phrases using different types of masks. They measured the resulting intelligibility and human judgements of speaker consistency. Taken together, work on this VQ-VAE architecture is promising for content-based privacy because it effectively separates content from other information in the speech signal. The VQ-VAE design is also useful for the privacy scenario that involves speech compression and transmission, discussed in the next section.

3. Content Privacy Scenarios

Content privacy extends to any situation where sensitive information is delivered using voice. In this section, we outline four prominent scenarios that are timely and relevant given the current state of the art for speech technology. There may be some overlap between the privacy needs of the scenarios, however it is possible that the technical solutions will vary.

3.1. Voice Storage Privacy

All voice-enabled devices capture and store speech data, and in some cases also transmit it from the device to a larger database on a remote computing server. Speech capture and storage will sometimes involve private conversations as a result of intentional or unintentional recordings. While some storage mechanisms have security measures by design, such as secure enclaves on mobile devices or data encryption, content-based privacy offers an additional layer of protection [16]. Numerous functionalities for voice-enabled devices require the ability to access stored voice content. Speech recognition on mobile devices is one example that requires storing speech data, though it is possible to fully encrypt all speech content while performing speech recognition [17]. In addition, it would be beneficial to create "edge" privacy solutions that can mask sensitive content on a device when the speech is first captured by the microphone, preferably also within a secure enclave. Successful content privacy could enable researchers to utilize speech databases for research and development that would otherwise be prohibited, due to legal issues with the European Union GDPR [18].

[2] https://clarin.phonetik.uni-muenchen.de/BASWebServices/interface

3.2. Speech Compression, Transmission, and Broadcast

In order to transmit or broadcast speech, it must undergo compression which creates a more compact representation of the data. This is true for mobile phones, internet voice calling, and television broadcast, among others. It is possible for an intruder to intercept, eavesdrop and even maliciously manipulate speech content during transmission. Watermarking has been proposed as a countermeasure solution [19]. However, watermarking only helps to ensure the message remains unchanged and it does not conceal sensitive content. Other countermeasures such as voice scramblers would require highly specialized hardware and software solutions, and some intelligibility may be lost during the scrambling and unscrambling process [20]. Related broadcast scenarios include law court testimony, emergency calls, and policing: it is important to protect the witness identity, which implies hiding or masking different levels of information, from voice identity to linguistic content. At the same time, it is important to retain other non-sensitive information as much as possible in order to provide valid testimony. Sensitive testimony may also require redaction before being released to the public or while it is being televised [21].

3.3. Speech and Speaker Recognition

As mentioned earlier, there is a trade-off between protecting sensitive content while also using the speech for downstream tasks such as ASR and speaker recognition. Certain speech technologies may require speaker information to remain unaltered by the content masking. Authentication by voice, also known as automatic speaker verification (ASV) [22], is a common application where the speaker information needs to be preserved when using content masking at the same time. ASV typically compares two utterances (a *reference* with a *test* utterance) to produce a score, subject to binary decision. The score is high if the two utterances likely come from the same speaker (*target* proposition) or the score is low if the utterances come from different speakers (*impostor* proposition). A related application is speaker diarization [23] which aims to detect *who spoke when?* in a multi-speaker conversation. Content masking can be used in this scenario if it does not alter speaker information or cause confusion between speakers.

3.4. Voice-Enabled Assistive Technology

When a user interacts with their voice assistant, such as Siri or Google, the responses spoken aloud from the device may contain sensitive information that the user does not want people nearby to overhear [7, 24, 25]. Blind users of speech technology face unique challenges for privacy when using the internet and they are some of the heaviest users of text-to-speech (TTS) synthesis since it is the core technology of screen-readers [26]. While sighted people can enjoy a particular amount of content privacy from quietly reading text on a screen, this type of privacy is not extended to blind users who must have screens read aloud using screen-reading software [27]. Focus groups show that in public spaces blind users may hold a device very close to their ear or use earbuds, even though this practice is potentially hazardous because it blocks out other environmental noises that blind users must attend to [28]. There are many nuances to developing speech technologies that are optimized for blind users. Content privacy is under-explored and could have a big impact for accessibility [29]. It may be possible to embed privacy capabilities within the TTS screen-reader, but that would prevent the user from receiving important information. Another possibility

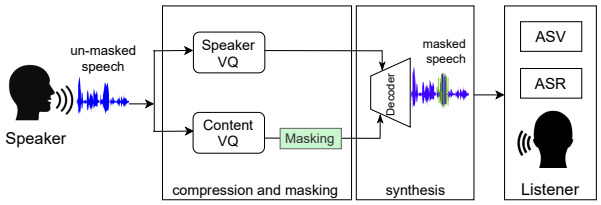

Figure 1: *Simultaneous speech compression and content masking using a deep learning technique called VQ-VAE.*

is to develop a special earbud customized for blind users, while allowing for other important sounds in the environment.

4. Privacy Approaches

Ideally, the solutions to content privacy would be optimized for the specific needs and requirements of each particular scenario. For example, a customized earbud for blind users of screen-readers can be very different from privacy solutions for speech databases. Even still, as far as speech is concerned there are some general approaches that are worth discussing as a starting point. Speech signal disentanglement stands out as a promising overall approach. Disentanglement is a form of distributed representation learning that separates different types of speech information into separate representations, such as speaker identity and speech content. One of the main benefits of disentanglement is that it allows content to be modified separately from other informational factors. In addition, some disentanglement techniques such as VQ-VAE also compress the speech signal, which is beneficial for transmission scenarios [14, 15]. The VQ-VAE approach is shown in Figure 1. Original, un-masked speech is disentangled into separate representations of speaker identity and content using two vector-quantized (VQ) codebooks. These codebooks are highly compressed The content VQ codebook is used for content masking. The masked speech is synthesized, and made available to human listeners or downstream speech technologies.

Speech content can be masked through various mechanisms and one of the most obvious would be to replace sensitive content with silence or noise. However, there have not yet been any studies to determine how different types of masks impact performance on downstream speech tasks such as ASR, ASV, or human listening effort and intelligibility. Another issue is whether or not a content mask would be reversible in the sense that the speech content could be concealed and later recovered. A reversible privacy mask might not be ideal for speech databases described in Section 3.1 if the speech data will be shared with third-parties. On the other hand, a reversible mask would be useful for speech transmission described in Section 3.2 where the goal may be to protect content from being intercepted only during transmission.

5. Content Privacy Evaluation

Currently there are no established protocols for evaluating speech content privacy. While it is not the goal of this paper to definitively specify an evaluation protocol, we present three assessment viewpoints that can help inform future efforts: task-based, high-level, and low-level.

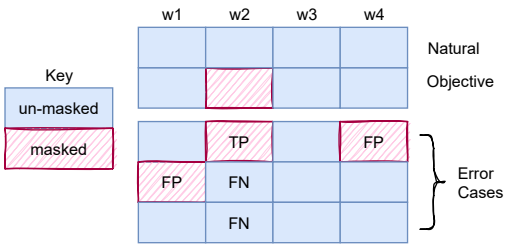

Figure 2: *Sample word-level masking errors and decisions which can be compared to natural (un-masked) and objective (with masking), where $w_1, w_2..w_n$ is a sequence of words.*

5.1. Task-Based Assessment

When applying ASV on content-masked speech it is important to ensure that speaker information is not altered. The speech output of a content masking system may not be perfect due to compression or the quality of speech vocoder. The result may be a speaker identity shift in the synthetic voice space, even for portions of speech without content masking such as surrounding words. Consequently, a natural and a content-masked utterance coming from the same speaker could be marked as two different speakers. One way to assess if content-masking has affected the speaker identity is to compare un-masked enrolment utterances with masked test utterances. Whereas to check speaker separability in the protected space, the enrolment and test utterances would both be masked. As explained in Section 3.3, an ASV system compares an enrolment and test utterance, and produces a similarity score. Then a threshold, also known as the operating point, is set in order to decide between the target and impostor propositions. There are two kinds of possible errors for the ASV system: false alarms (FA) and false rejections (FR). Several metrics are used to interpret these errors. The equal error rate (EER) describes the operating point at which the FA and the FR rates are equal. The log-likelihood-ratio cost [30] is also commonly used to evaluate ASV systems. It measures the ability of the scores to resemble calibrated log-likelihood-ratios (LLRs) and is thus independent of the operating point.

Content-masking can also be evaluated in terms of an ASR-style task, especially for privacy scenarios that require high intelligibility for the un-masked and non-sensitive surrounding words. A word error rate (WER) or phone error rate (PER) measures how many words or phones are correctly recognised by an ASR system. The WER/PER should decline proportionally with the quantity of words that have been masked. Human judgements of intelligibility have similar requirements. One way to assess the impacts on ASR and intelligibility is to present human listeners with masked speech audio alongside ASR output and measure how often listeners agree with the ASR transcript based on what they hear [13]. This hybrid style of aligning human judgements with task-based performance holds for ASR as well as ASV and speaker separation.

5.2. High-Level Assessment

This paper has been discussing content privacy based on the notion that *content* refers to spoken words. For speech privacy and security, different types of word mask errors imply different consequences. For example, failing to mask a target sensitive phrase might invoke a penalty whereas accidentally masking a non-sensitive phrase would not. As discussed earlier, some privacy scenarios require that non-sensitive words remain highly

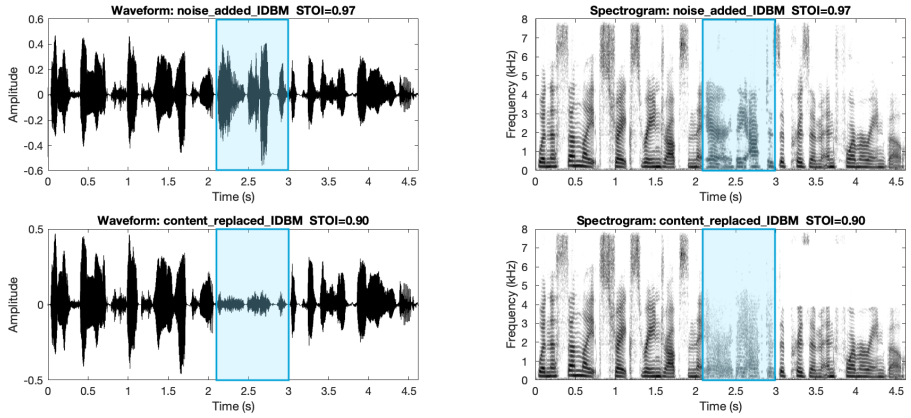

Figure 3: *Waveform and spectrogram to compare ideal binary mask from two different content-masking approaches: additive noise (top) and replacement with noise (bottom). In each case, target content to be masked is highlighted by the green box. "When sunlight strikes raindrops in the* ***[air they act as a]*** *prism and form a rainbow."*

intelligible for human listeners or for other speech technologies like ASR. We introduce a metric called *mask error rate* (MER) which can be used specifically to assess errors about which words have been masked correctly. Consider four types of errors/decisions (Figure 2) at the word-level: True negative (TN) word is correctly unmasked; True positive (TP) word is correctly masked; False negative (FN) word is incorrectly unmasked; False positive (FP) word is incorrectly masked.

The MER metric can be described by Equation 1. For a given utterance, the weighted combination of masking errors with respect to the length of the utterance:

$$MER_{utt} = \frac{\alpha FN + \beta FP}{TN + TP + FN + FP} \quad (1)$$

where α and β are penalties that can be used to balance the two types of word masking errors. For speech privacy, an FN error may need to be weighted more heavily because it could lead to revealing sensitive information. This metric could be adapted for any size of chunk, larger or smaller than the word level. One potential limitation is that MER requires high-quality time alignments in order to perform the calculations. To be useful in practice, MER should also account for slight variation of word boundaries, such as inadvertently causing surrounding words to become unintelligible. For reversible masking, MER can be adapted to measure how much content is recoverable when the mask is reversed.

5.3. Low-Level Assessment

It may also be possible to develop an evaluation metric borrowing from a technique in speech enhancement, called *ideal binary masks*. An idea binary mask is used to remove various types of noise from the speech signal (babble, static, reverberation, etc). There are many different versions of this technique. Overall it can be summarized as comparing the original clean signal with a noisy corrupted signal, and computing signal-to-noise ratio (SNR) to identify which areas of the speech signal could be attenuated. This effectively removes the noise portions of the signal, while leaving the speech portions of the signal intact. An ideal binary mask describes the perfect (*idealized*) solution of removing noise in the speech signal so that the noise (and only the noise) is completely removed, while also preserving speech intelligibility [31].

Consider two versions of speech processed with an ideal binary mask shown as waveforms and spectrograms in Figure 3 [32]. The top was created by *adding* a temporally-modulated speech-shaped noise masker (ICRA noise 9 from [33]) to the signal, to mask a target phrase, and then an ideal binary mask was calculated and applied to attempt to recover the speech. The bottom was created by *replacing* a target phrase with the same type of noise. Recovery of the target phrase can be measured by a short term objective intelligibility measure (STOI)[3]. The STOI value for the additive noise is higher than the replacement noise, indicating that the target phrase is more recoverable when masked with additive noise.

6. Discussion and Future Work

We have discussed some of the current issues surrounding speech content privacy. While some of the scenarios for this capability will require slightly different solutions to be implemented, speech disentanglement is a promising overarching approach because it isolates speech content from other information in the speech signal. New progress in speech content privacy will be timely due to very recent advances in machine learning. It will have a large impact on society since privacy concerns influence how people adopt new voice technologies. One of the most important technical challenges will be processing privacy in real-time, and in a way that balances privacy needs with freedoms of expression. Allowing users a mechanism to adjust and control their content privacy settings will help create this necessary balance. Privacy controllability would allow users to have different privacy features in different settings, such as at home versus in public, or depending on who is nearby, or the type of voice device being used.

7. Acknowledgements

This work was partially supported by the EPSRC Centre for Doctoral Training in Data Science, funded by the UK Engineering and Physical Sciences Research Council (grant EP/L016427/1) and University of Edinburgh; and by a JST CREST Grant (JPMJCR18A6, VoicePersonae project), Japan.

[3]https://github.com/mpariente/pystoi

8. References

[1] M. AKAGI and Y. IRIE, "Privacy Protection for Speech Based on Concepts of Auditory Scene Analysis," *Proc. INTERNOISE 2012*, p. 485, 2012.

[2] K. Kondo and H. Sakurai, "Gender-Dependent Babble Maskers Created From Multi-Speaker Speech for Speech Privacy Protection," in *2014 Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*. IEEE, 2014, pp. 251–254.

[3] J. Donley, C. Ritz, and W. B. Kleijn, "Improving Speech Privacy in Personal Sound Zones," in *2016 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 2016, pp. 311–315.

[4] C. Phunruangsakao, P. Kraikhun, S. Duangpummet, J. Karnjana, M. Unoki, and W. Kongprawechnon, "Speech Privacy Protection Based on Controlling Estimated Speech Transmission Index," in *2020 17th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON)*. IEEE, 2020, pp. 628–631.

[5] A. Nautsch, A. Jiménez, A. Treiber, J. Kolberg, C. Jasserand, E. Kindt, H. Delgado, M. Todisco, M. A. Hmani, A. Mtibaa *et al.*, "Preserving Privacy in Speaker and Speech Characterisation," *Computer Speech & Language*, vol. 58, pp. 441–480, 2019.

[6] J. A. Blumenthal, M. Adya, and J. Mogle, "The Multiple Dimensions of Privacy: Testing Lay 'Expectations of Privacy'," *University of Pennsylvania Journal of Constitutional Law*, vol. 11, no. 2, p. 331, 2009.

[7] M. Vimalkumar, S. K. Sharma, J. B. Singh, and Y. K. Dwivedi, "'okay Google, what about my privacy?': User's Privacy Perceptions and Acceptance of Voice Bbased Digital Assistants," *Computers in Human Behavior*, vol. 120, p. 106763, 2021.

[8] Q. Yang, Y. Liu, Y. Cheng, Y. Kang, T. Chen, and H. Yu, "Federated Learning," *Synthesis Lectures on Artificial Intelligence and Machine Learning*, vol. 13, no. 3, pp. 1–207, 2019.

[9] A. van den Oord, S. Dieleman, H. Zen, K. Simonyan, O. Vinyals, A. Graves, N. Kalchbrenner, A. Senior, and K. Kavukcuoglu, "Wavenet: A Generative Model for Raw Audio," in *9th ISCA Speech Synthesis Workshop*, 2016, pp. 125–125.

[10] N. Kalchbrenner, E. Elsen, K. Simonyan, S. Noury, N. Casagrande, E. Lockhart, F. Stimberg, A. Oord, S. Dieleman, and K. Kavukcuoglu, "Efficient Neural Audio Synthesis," in *International Conference on Machine Learning*. PMLR, 2018, pp. 2410–2419.

[11] J. Ebbers, M. Kuhlmann, T. Cord-Landwehr, and R. Haeb-Umbach, "Contrastive Predictive Coding Supported Factorized Variational Autoencoder for Unsupervised Learning of Disentangled Speech Representations," in *ICASSP 2021-2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 2021, pp. 3860–3864.

[12] J. Williams, Y. Zhao, E. Cooper, and J. Yamagishi, "Learning Disentangled Phone and Speaker Representations in a Semi-Supervised VQ-VAE Paradigm," in *ICASSP 2021-2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 2021, pp. 7053–7057.

[13] M. A. T. Turan, D. Klakow, E. Vincent, and D. Jouvet, "Adapting Language Models When Training on Privacy-Transformed Data," in *INTERSPEECH 2021*, 2021.

[14] J. Casebeer, V. Vale, U. Isik, J.-M. Valin, R. Giri, and A. Krishnaswamy, "Enhancing into the Codec: Noise Robust Speech Coding with Vector-Quantized Autoencoders," in *ICASSP 2021-2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 2021, pp. 711–715.

[15] J. Williams, J. Fong, E. Cooper, and J. Yamagishi, "Exploring Disentanglement with Multilingual and Monolingual VQ-VAE," *Speech Synthesis Workshop (SSW11)*, 2021.

[16] J. Qian, F. Han, J. Hou, C. Zhang, Y. Wang, and X.-Y. Li, "Towards privacy-preserving speech data publishing," in *IEEE INFOCOM 2018-IEEE Conference on Computer Communications*. IEEE, 2018, pp. 1079–1087.

[17] C. Glackin, G. Chollet, N. Dugan, N. Cannings, J. Wall, S. Tahir, I. G. Ray, and M. Rajarajan, "Privacy preserving encrypted phonetic search of speech data," in *2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 2017, pp. 6414–6418.

[18] A. Nautsch, C. Jasserand, E. Kindt, M. Todisco, I. Trancoso, and N. Evans, "The GDPR & Speech Data: Reflections of Legal and Technology Communities, First Steps Towards a Common Understanding," in *Proceedings of the Annual Conference of the International Speech Communication Association, INTERSPEECH*. ISCA, 2019.

[19] O. T.-C. Chen and C.-H. Liu, "Content-Dependent Watermarking Scheme in Compressed Speech with Identifying Manner and Location of Attacks," *IEEE Transactions on audio, speech, and language processing*, vol. 15, no. 5, pp. 1605–1616, 2007.

[20] J. F. de Andrade, M. L. de Campos, and J. A. Apolinario, "Speech privacy for modern mobile communication systems," in *2008 IEEE International Conference on Acoustics, Speech and Signal Processing*. IEEE, 2008, pp. 1777–1780.

[21] R. E. Roberts Jr, "An Empirical and Normative Analysis of the Impact of Televised Courtroom Proceedings," *SMU Law Review*, vol. 51, no. 3, p. 621, 1998.

[22] F. Bimbot, J.-F. Bonastre, C. Fredouille, G. Gravier, I. Magrin-Chagnolleau, S. Meignier, T. Merlin, J. Ortega-García, D. Petrovska-Delacrétaz, and D. A. Reynolds, "A Tutorial on Text-Independent Speaker Verification," *EURASIP Journal on Advances in Signal Processing*, vol. 2004, no. 4, pp. 1–22, 2004.

[23] X. Anguera, S. Bozonnet, N. Evans, C. Fredouille, G. Friedland, and O. Vinyals, "Speaker Diarization: A Review of Recent Research," *IEEE Transactions on Audio, Speech, and Language Processing*, vol. 20, no. 2, pp. 356–370, 2012.

[24] A. Easwara Moorthy and K.-P. L. Vu, "Privacy Concerns for Use of Voice Activated Personal Assistant in the Public Space," *International Journal of Human-Computer Interaction*, vol. 31, no. 4, pp. 307–335, 2015.

[25] Y. Liao, J. Vitak, P. Kumar, M. Zimmer, and K. Kritikos, "Understanding the Role of Privacy and Trust in Intelligent Personal Assistant Adoption," in *International Conference on Information*. Springer, 2019, pp. 102–113.

[26] G. Regal, E. Mattheiss, M. Busch, and M. Tscheligi, "Insights into Internet Privacy for Visually Impaired and Blind People," in *International Conference on Computers Helping People with Special Needs*. Springer, 2016, pp. 231–238.

[27] A. Abdolrahmani, R. Kuber, and S. M. Branham, "'siri Talks at You' An Empirical Investigation of Voice-Activated Personal Assistant (VAPA) Usage by Individuals who are Blind," in *Proceedings of the 20th International ACM SIGACCESS Conference on Computers and Accessibility*, 2018, pp. 249–258.

[28] M. Podsiadło and S. Chahar, "Text-to-Speech for Individuals With Vision Loss - A User Study." in *Interspeech 2016*, 2016.

[29] B. Kuriakose, R. Shrestha, and F. E. Sandnes, "Tools and Technologies for Blind and Visually Impaired Navigation Support: A Review," *IETE Technical Review*, pp. 1–16, 2020.

[30] N. Brümmer and J. du Preez, "Application-Independent Evaluation of Speaker Detection," *Computer Speech & Language*, vol. 20, no. 2, pp. 230–275, 2006, odyssey 2004: The speaker and Language Recognition Workshop. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0885230805000483

[31] P. C. Loizou and G. Kim, "Reasons Why Current Speech-Enhancement Algorithms do not Improve Speech Intelligibility and Suggested Solutions," *IEEE transactions on audio, speech, and language processing*, vol. 19, no. 1, pp. 47–56, 2010.

[32] K. Wojcicki. Ideal Binary Mask. [Online]. Available: https://www.mathworks.com/matlabcentral/fileexchange/33199-ideal-binary-mask

[33] M. Cooke, C. Mayo, C. Valentini-Botinhao, Y. Stylianou, B. Sauert, and Y. Tang, "Evaluating the intelligibility benefit of speech modifications in known noise conditions," *Speech Communication*, vol. 55, no. 4, pp. 572–585, 2013.