Audio Security & Privacy

Andreas Nautsch, Massimiliano Todisco, Jose Patino, Nicholas Evans

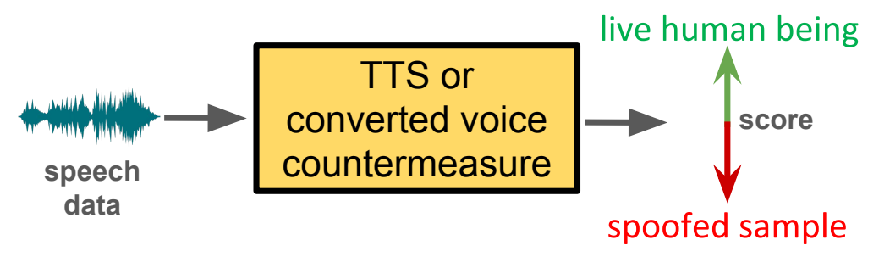
Audio Security and Privacy Research Group, Digital Security Department, EURECOM, France

Abstract

- Overview of the audio security and privacy lab at EURECOM
- Speech is part of daily life: smart speakers, virtual assistants, ...
- Speech as a medium to seamlessly impart and exchange information
  - Personal assistants
  - Smart home
  - Call centers
  - Online banking
  - Health care
  - Forensic sciences, ...
- Threats
  - Repurposing speech data: threat of privacy infringement
  - Subversion system security: countermeasures?

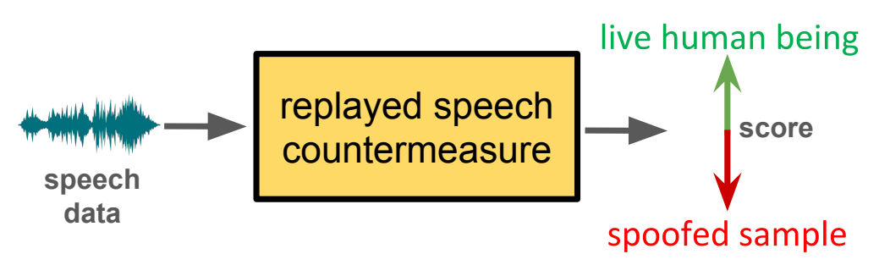
Security: Automatic Speaker Verification Anti-Spoofing (ASVspoof) Challenges

ASVspoof 2015



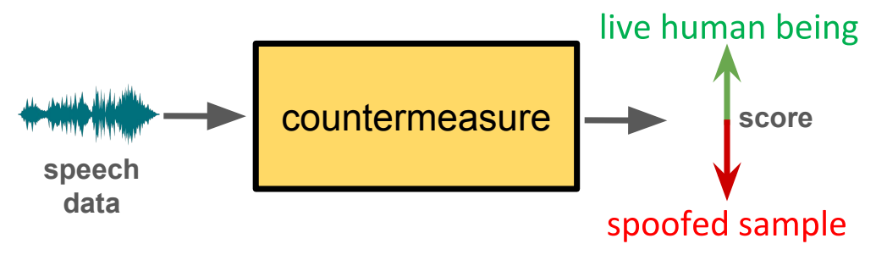
16 organizations participated

ASVspoof 2017

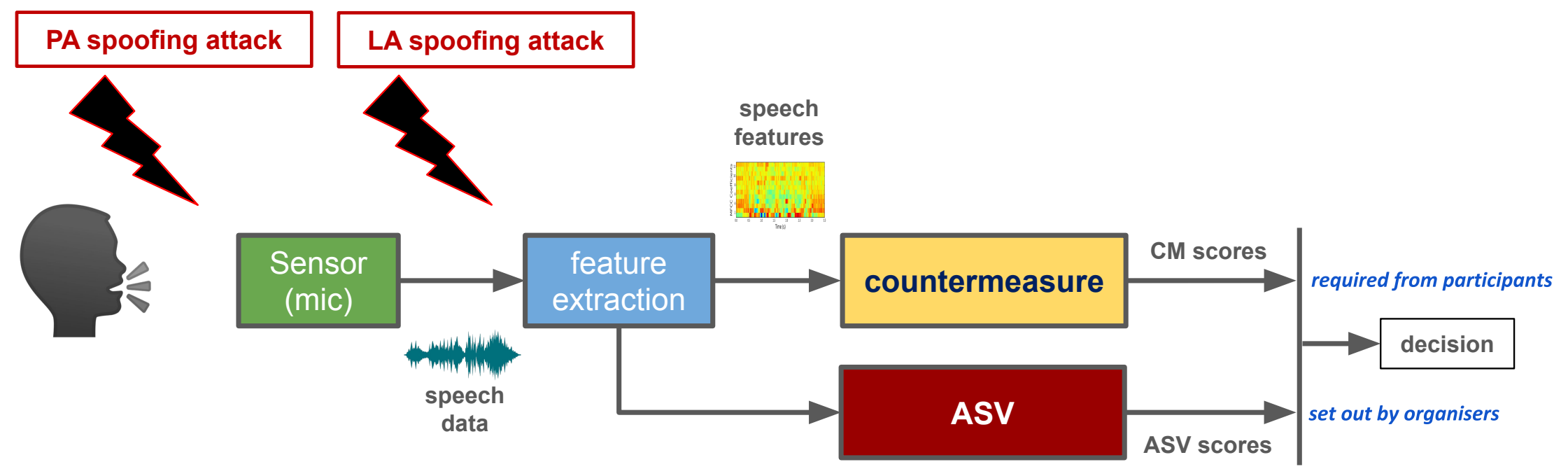


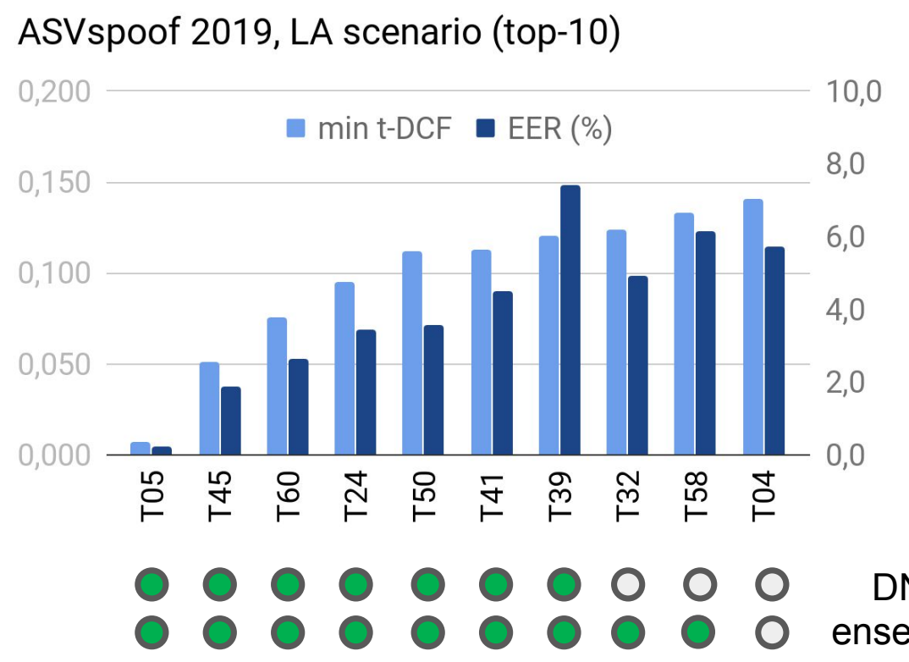
49 organizations participated

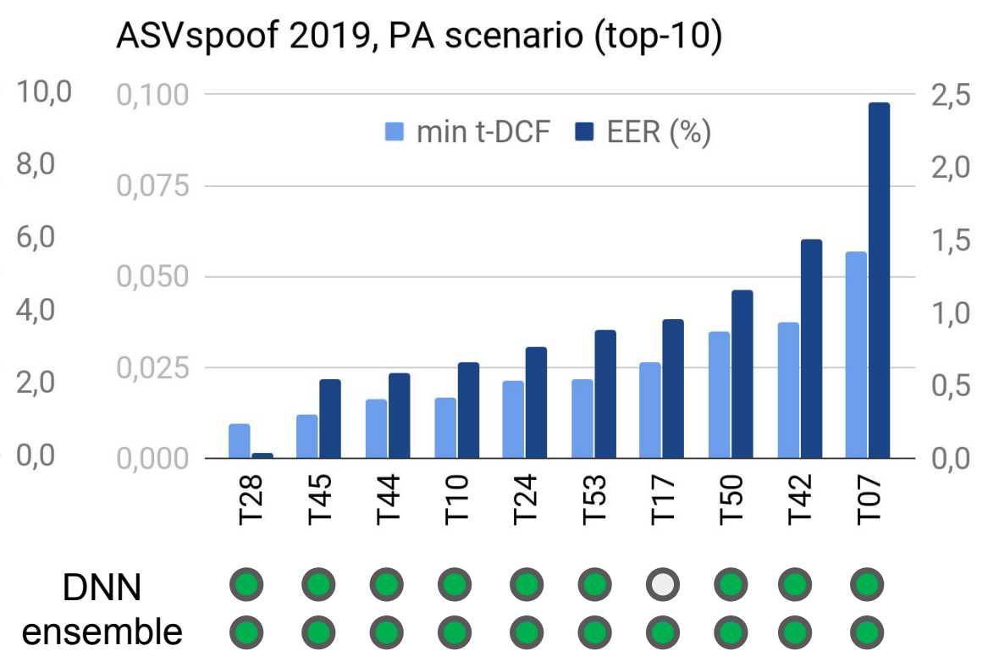
ASVspoof 2019

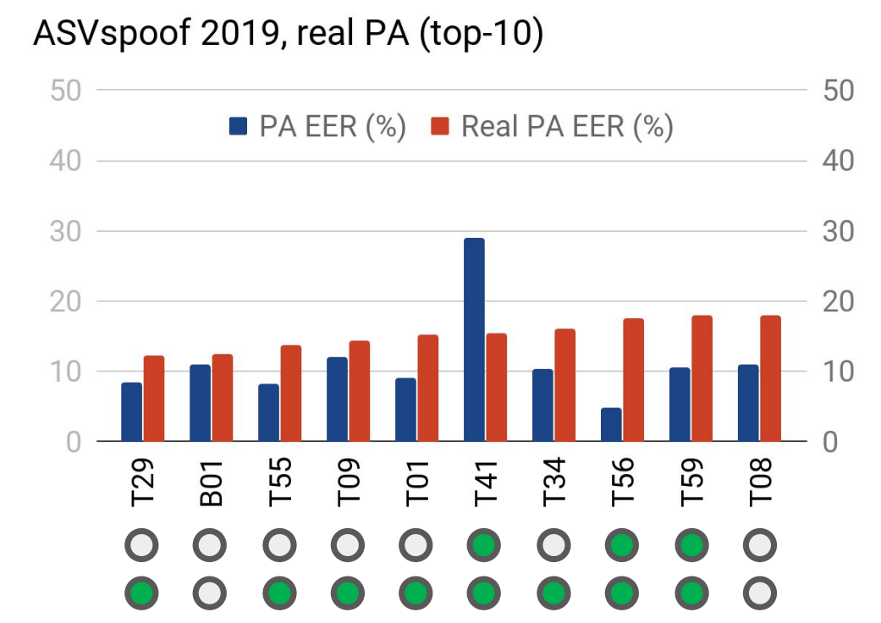


154 teams participated





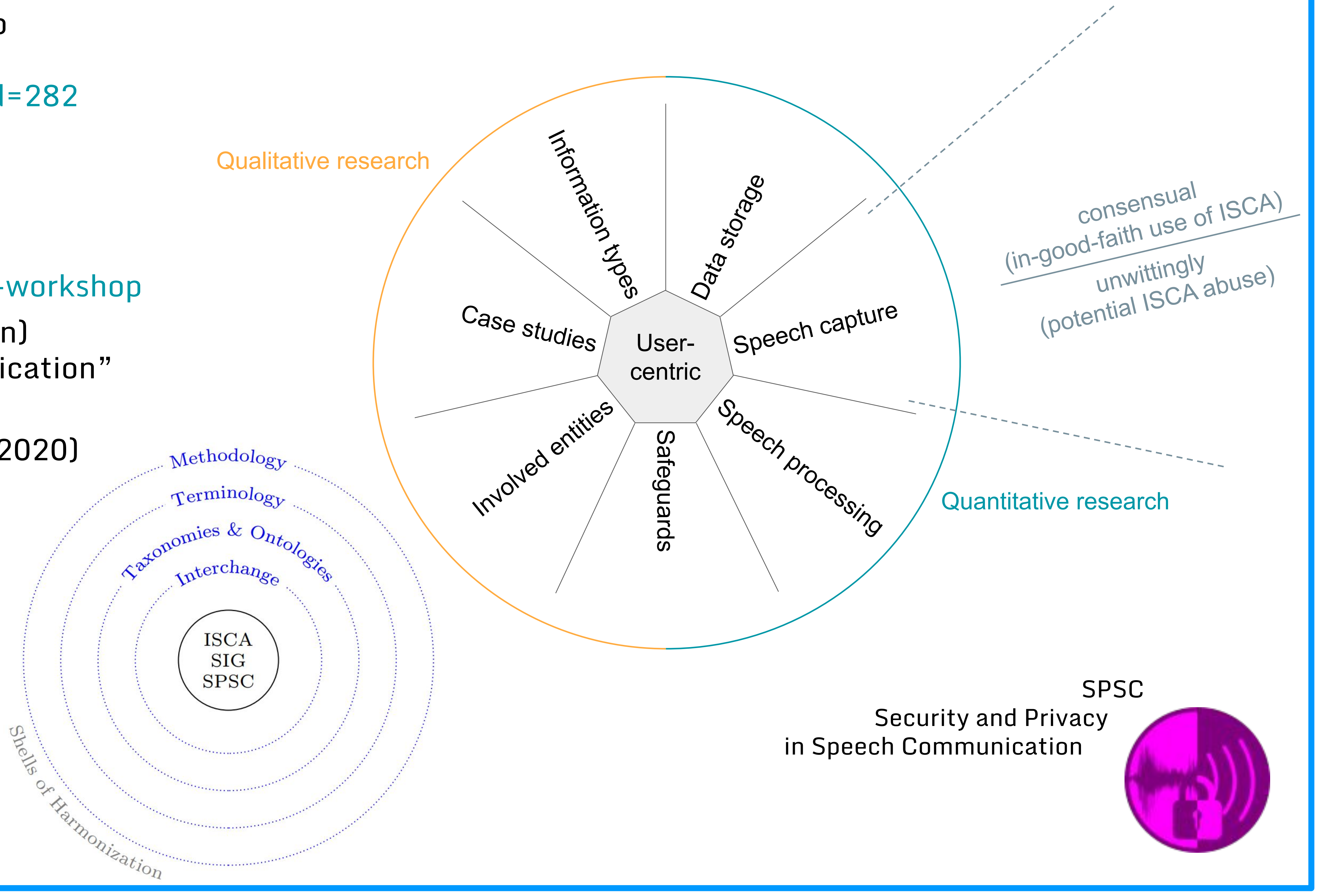




"hidden track" of ASVspoof 2019

Privacy in Speech Communication

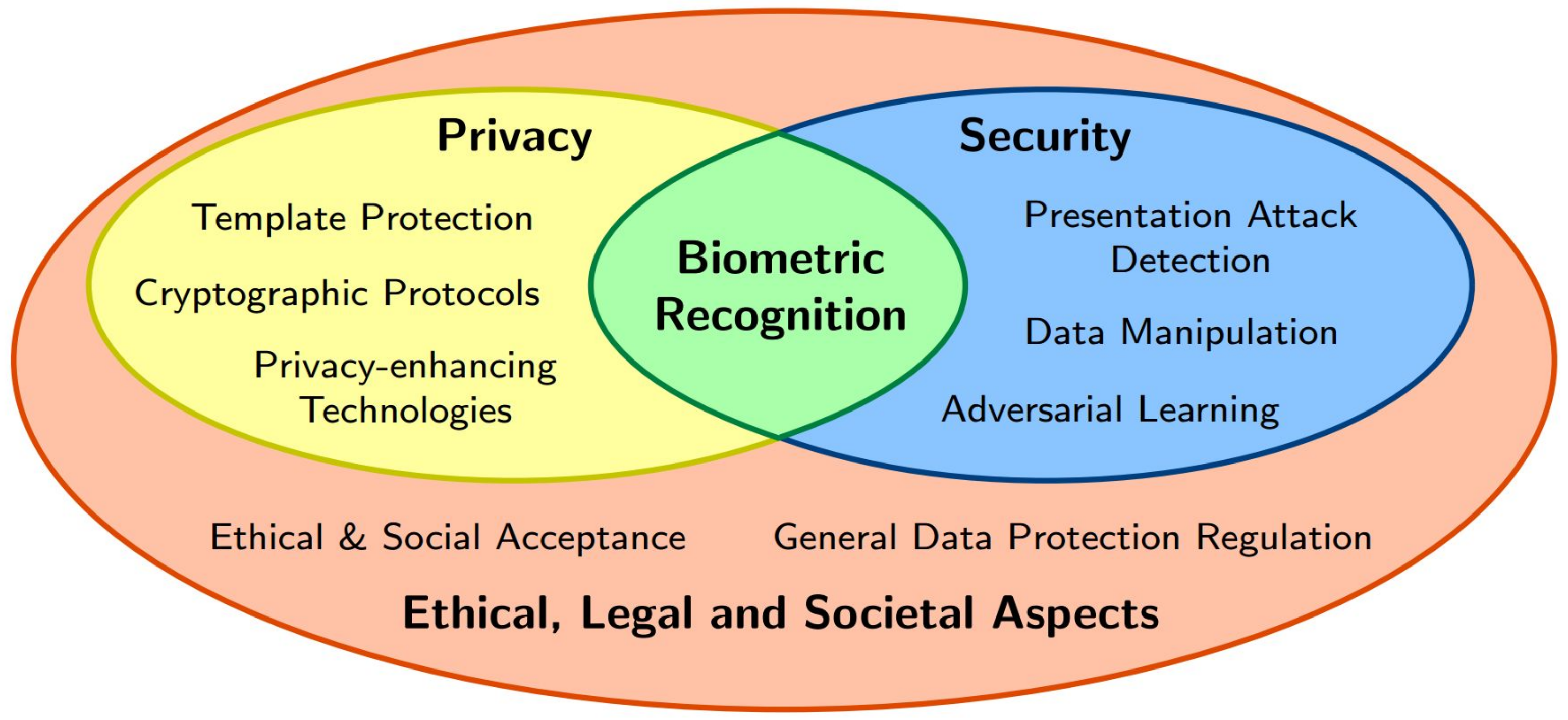
- Co-funding and co-leading ISCA Special Interest Group "Security & Privacy in Speech Communication"
  https://www.isca-speech.org/iscaweb/index.php/sigs?id=282
  LinkedIn: https://www.linkedin.com/groups/13808029
  Mailing list: list@spsc-sig.org
  - Co-organizing: concept workshop "Privacy: Speech meets Legal experts"
    https://www.spsc-sig.org/2020-01-29-speech-legal-workshop
  - Co-organizing: Dagstuhl-style Shonan seminar (Japan) "Privacy, Ethics, and Legislation for Speech Communication"
    https://shonan.nii.ac.jp/seminars/170
  - Co-organizing: VoicePrivacy challenge (Interspeech 2020)
    https://www.voiceprivacychallenge.org
- Inter-disciplinary research
  - Speech communication
  - Ethics & study of the Law
  - Human computer interfaces with speech as medium
  - Cybersecurity: cryptography & secure computation
- Next steps - collaborative drafting:
  - Webinar follow-up to Shonan meeting (open)
  - Research roadmap "10+ years"
  - Code of conduct



SPSC
Security and Privacy
in Speech Communication

TReSPAsS-ETN (MSCA-ITN 2020-2023)

- Multi-biometrics (voice, softbiometrics, fingerprint, face & iris)
- Privacy-preserving biometric technologies
  - Protection of biometric templates, models & information
  - Application & evaluation of cryptographic techniques
- Security protection in biometric systems
  - Assessment: biometric presentation & morphing attacks
  - Attack detection & integration of solutions
- Ethical, logal and societal acceptance issues surrounding biometrics
  - Requirement proposal for data protection & security in biometrics
  - Development: regulatory framework to assess requirements


Privacy
Template Protection
Cryptographic Protocols
Privacy-enhancing Technologies
Biometric Recognition
Security
Presentation Attack Detection
Data Manipulation
Adversarial Learning
Ethical & Social Acceptance
General Data Protection Regulation
Ethical, Legal and Societal Aspects

References

[Bayerl+19] Privacy-preserving speech processing via STPC and TEEs, Privacy Preserving Machine Learning Workshop, CCS 2019 Workshop, 2019

[Nautsch+19a] Preserving privacy in speaker and speech characterisation, Computer Speech & Language, Vol. 58, November 2019

[Nautsch+19b] The GDPR & speech data: Reflections of legal and technology communities, first steps towards a common understanding, INTERSPEECH, 2019

[Patino19] Efficient speaker diarization and low-latency speaker spotting, PhD Thesis, EURECOM, 201

[Sahidullah+19] The SPEED submission to DIHARD II: Contributions and lessons learned, Idiap-RR-14-2019, Idiap Research Report, 2019

[Todisco+19] ASVspoof 2019: Future horizons in spoofed and fake audio detection, INTERSPEECH, 2019

[Wang+19] The ASVspoof 2019 database, arXiv:1911.01601v1, 2019

Acknowledgments

This work is partially funded by the EU H2020 research and innovation programme under the MSCA grant agreement No. 860813 (TReSPAsS-ETN), the ANR-DFG French-German joint project ANR-18-CE92-0024 (RESPECT), the ANR project ANR-19-DATA-0008 (HARPOCRATES), the ANR project ExTENSoR and the JST-ANR Japanese-French project VoicePersonae.