2020.07.05

THE OPEN VOICE NETWORK AND PRIVACY

A 1.0 Primer for OVN Committees and Communities

TABLE OF CONTENTS

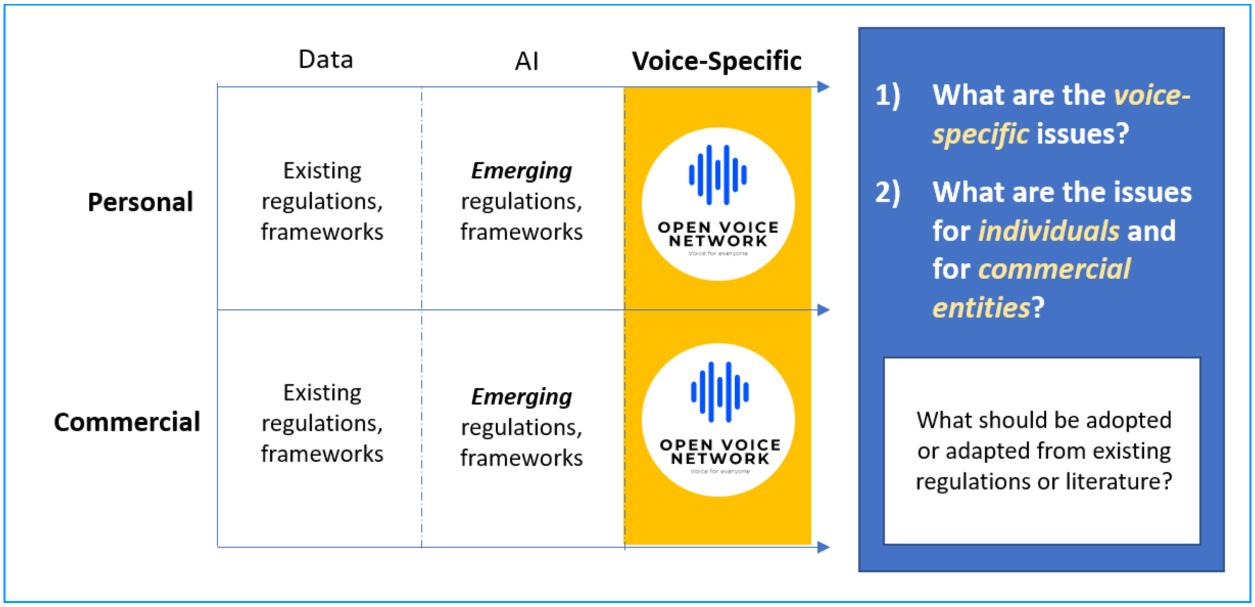
INTRODUCTION

The issue of privacy is central to the work of The Open Voice Network.

In its development of technical standards and ethical use guidelines, it must address the topic from two critical perspectives within an understanding of the technologies and systems of today's and tomorrow's conversational AI:

- The issues of privacy that are ***unique*** to voice assistance;
- The issues of voice assistance privacy for ***individuals*** and for ***commercial entities.***

Below is an at-a-glance framework for OVN deliberation and decision-making in regards to privacy.



	Data	AI	**Voice-Specific**
Personal	Existing regulations, frameworks	***Emerging*** regulations, frameworks	OPEN VOICE NETWORK Voice for everyone
Commercial	Existing regulations, frameworks	***Emerging*** regulations, frameworks	OPEN VOICE NETWORK Voice for everyone

1) What are the *voice-specific* issues?

2) What are the issues for *individuals* and for *commercial entities*?

What should be adopted or adapted from existing regulations or literature?

As address these issues, it is essential that The Open Voice Network understand current regulation, legislation, and academic research on the topic of privacy.

Thus, this primer, which is of two parts:

- Privacy definitions, from NIST, GDPR, and CCPA
- Ethical Use framework commentary which includes privacy.

1 PRIVACY DEFINITIONS

U.S. DEPARTMENT OF COMMERCE: NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

From the NIST Privacy Framework 1.0 (2020.01.16)
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf

Privacy definitions.

Definition(s):
Restricting access to subscriber or Relying Party information in accordance with Federal law and Agency policy.
Source(s):
NIST SP 800-32 under Privacy

Freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue or illegal gathering and use of data about that individual
Source(s):
NISTIR 8053 ISO/IEC 2382

The right of a party to maintain control over and confidentiality of information about itself.
Source(s):
NISTIR 4734 under Privacy

Privacy is challenging because not only is it an all-encompassing concept that helps to safeguard important values such as human autonomy and dignity, but also the means for achieving it can vary. For example, privacy can be achieved through seclusion, limiting observation, or individuals' control of facets of their identities (e.g., body, data, reputation). Moreover, human autonomy and dignity are not fixed, quantifiable constructs; they are filtered through cultural diversity and individual differences. This broad and shifting nature of privacy makes it difficult to communicate clearly about privacy risks within and between organizations and with individuals. What has been missing is a common language and practical tool that is flexible enough to address diverse privacy needs.

EUROPEAN UNION: GENERAL DATA PROTECTION REGULATIONS (GDPR)

https://gdpr.eu/data-privacy/?cn-reloaded=1

Privacy definitions.

Chapter 3 of the GDPR lays out the data privacy rights and principles that all "natural persons" are guaranteed under EU law. As an organization, you are obligated to facilitate these rights. Failure to do so can result in penalties (see "**GDPR fines**"). Here's a very basic summary of each of the articles under Chapter 3.

Article 12 — Transparency and communication
Read GDPR Article 12

You have to explain how you process data in "a concise, transparent, intelligible and easily accessible form, using clear and plain language" (see "**privacy notice**"). You must also make it easy for people to make requests to you (e.g., a right to erasure request, etc.) and respond to those requests quickly and adequately.

Articles 13 & 14 — When collecting personal data
Read GDPR Article 13
Read GDPR Article 14

At the moment you collect **personal data** from a user, you need to communicate specific information to them. If you don't collect the information directly from the user, you are still required to provide them with similar information. These articles list the exact information you have to provide.

Article 15 — Right of access
Read GDPR Article 15

Data subjects have the right to know certain information about the processing activities of a data controller. This information includes the source of their personal data, the purpose of processing, and the length of time the data will be held, among other items. Most importantly, they have a right to be provided with the personal data of theirs that you're processing.

Article 16 — Accuracy
Read GDPR Article 16

The accuracy of the data you process is only tangentially an aspect of data privacy, but people have a right to correct inaccurate or incomplete personal data that you are processing.

Article 17 — Right to erasure
Read GDPR Article 17

Also known as the "**right to be forgotten**," data subjects have the right to request that you delete any information about them that you have. There are five exemptions to this right, including when processing their data is necessary to exercise your right to freedom of expression. You must make it simple for data subjects to file right to erasure requests. You can find a template for such requests **here**.

Article 18 — Right to restrict processing
Read GDPR Article 18
Read GDPR Article 19

Short of asking you to erase their data, data subjects can request that you temporarily change the way you process their data (**such as removing it temporarily from your website**) if they believe the information is inaccurate, is being used illegally, or is no longer needed by the controller for the purposes claimed. The data subject has the right to simply object to your processing of their data as well. Also important to note: If you decide to take any action related to Articles 16, 17, or 18, then Article 19 requires you to notify the data subject.

Article 20 — Data portability
Read GDPR Article 20

Remember that data privacy is the measure of control that people have over who can access their personal information. In line with this principle, the GDPR contains a novel data privacy requirement known as data portability. Basically, you have to store your users' personal data in a format that can be easily shared with others and understood. Moreover, if someone asks you to send their data to a designated third party, you have to do it (**if technically feasible**), even if it's one of your competitors.

Article 21 — Right to object
Read GDPR Article 21

Data subjects have the right to object to you processing their data. You can only override their objection by demonstrating the **legitimate basis** for using their data.

Final thoughts on data privacy

As you can see, the data privacy principles of the GDPR are fairly straightforward. The law asks you to make a good faith effort to give people the means to control how their data is used and who has access to it. To facilitate this, you must transparently and openly provide them with the information they need to understand how their data is collected and used. And you have to make it simple for your customers and users to exercise the various rights (of access, of erasure, etc.) contained in Chapter 3.

EU IT commentary on GDPR privacy definitions.

https://www.itgovernance.eu/blog/en/the-gdpr-what-exactly-is-personal-data

The GDPR: What exactly is personal data?

Luke Irwin 1st January 2020

- Personal data is at the heart of the GDPR (General Data Protection Regulation), but many people are still unsure exactly what 'personal data' refers to. There's no definitive list of what is or isn't personal data, so it all comes down to properly interpreting the GDPR's definition:
- Personal data' means any information relating to an identified or identifiable natural person ('data subject').

In other words, any information that is clearly about a particular person. But just how broadly does this apply? The GDPR clarifies:

- [A]n identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- That's an awful lot of information. In certain circumstances, someone's IP address, hair colour, job or political opinions could be considered personal data.
- The qualifier 'certain circumstances' is worth highlighting, because whether information is considered personal data often comes down to the context in which data is collected.

CONTEXT IS EVERYTHING

- Organisations usually collect many different types of information on people, and even if one piece of data doesn't individuate someone, it could become relevant alongside other data.
- For example, an organisation that collects information on people who download products from their website might ask them to state their occupation.

- This doesn't fall under the GDPR's scope of personal data, because, in all likelihood, a job title isn't unique to one person. Similarly, an organisation might ask what company they work for, which, again, couldn't be used to identify someone unless they were the only employee.

CALIFORNIA CONSUMER PROTECTION ACT (CCPA)

California Consumer Privacy Act Guide - Jones Day

Commentary on CCPA privacy definitions from global law firm Jones Day.

On June 28, 2018, California enacted the California Consumer Privacy Act ("CCPA")—the result of a last-minute compromise between California lawmakers and consumer privacy activists intended to avoid a widely criticized data privacy ballot initiative. The law, which is scheduled to go into effect on January 1, 2020, was amended in September 2018 and is likely to be modified again prior to the effective date. In its current form, the CCPA articulates certain data privacy rights of California residents, seeks to protect those rights by imposing new obligations on companies doing business in California, and grants the California Attorney General broad authority to implement related regulations. Specifically, the CCPA enumerates the following five rights of California consumers:

1. The right to know what consumer personal information is collected by businesses.
2. The right to know whether the personal information is sold or disclosed, and to whom such information is sold or disclosed.
3. The right to say no to the sale of personal information.
4. The right to access the personal information.
5. The right to equal service and price, even if privacy rights are invoked. The key provisions of the law require companies to respond to certain consumer requests regarding the collection and sale of their personal information. Importantly, the CCPA also provides consumers with a private right of action and statutory damages, in the event that certain unencrypted or unredacted personal information is subject to an unauthorized access and exfiltration, theft, or disclosure, as the result of a company's failure to implement and maintain reasonable security procedures and practices. In addition, the statute gives the attorney general the power to impose substantial penalties for violations of the statute, even if those violations do not result in a data breach.

Our experience counseling clients regarding the European Union's General Data Protection Regulation ("GDPR") suggests that successful compliance starts with substantial planning, preparation, and action prior to a law's effective date

The CCPA's definition of PI encompasses not only the data elements typically regarded as personal information in most data breach notification statutes (such as name and Social Security number), but also includes data such as physical characteristics, biometric information, online identifiers, and aspects of a consumer's Internet activity. Highlights of CCPA's List of Data Elements That Constitute "Personal Information"

- Identifiers, such as a real name, alias, postal address, unique personal identifier, online identifier, IP address, email address, account name, Social Security number, driver's license number, passport number, or other similar identifiers;
- Characteristics of protected classifications under California or federal law;
- Commercial information, including records of personal property, products or services purchased, obtained or considered, or other purchasing or consuming histories or tendencies;
- Biometric information;
- Internet or other electronic network activity information, including, but not limited to: browsing history, search history, and information regarding a consumer's interaction with a website, application, or advertisement;
- Geolocation data;
- Audio, electronic, visual, thermal, olfactory, or similar information;
- Professional or employment-related information;
- Education information, defined as information that is not publicly available or personally identifiable, as defined in the Family Educational Rights and Privacy Act (20 U.S.C. §1232g, 34 C.F.R. Part 99);
- Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics.

2 REGARDING AI ETHICAL USE

EUROPEAN UNION: ARTIFICIAL INTELLIGENCE, EXCELLENCE, AND TRUST

https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en

This February 2020 White Paper from The European Union speaks to an aspiration that – when translated to Voice Assistance – The Open Voice Network may wish to adopt.

Regarding a future regulatory framework for AI in Europe that will create a unique 'ecosystem of trust.'

. . . To do so, it must ensure compliance with EU rules, including the rules protecting fundamental rights and consumers' rights, in particular for AI systems operated in the EU that pose a high risk. Building an ecosystem of trust is a policy objective in itself, and should give citizens the confidence to take up AI applications and give companies and public organisations the legal certainty to innovate using AI. The Commission strongly supports a human-centric approach based on the Communication on Building Trust in Human-Centric AI8 and will also take into account the input obtained during the piloting phase of the Ethics Guidelines prepared by the High-Level Expert Group on AI.

On that basis, it can develop an AI ecosystem that brings the benefits of the technology to the whole of European society and economy:

- for **citizens** to reap new benefits for example improved health care, fewer breakdowns of household machinery, safer and cleaner transport systems, better public services;
- for **business** development, for example a new generation of products and services in areas where Europe is particularly strong (machinery, transport, cybersecurity, farming, the green and circular economy, healthcare and high-value added sectors like fashion and tourism); and
- for services of **public interest**, for example by reducing the costs of providing services (transport, education, energy and waste management), by improving the sustainability of products4 and by equipping law enforcement authorities with appropriate tools to ensure the security of citizens5, with proper safeguards to respect their rights and freedoms.

Given the major impact that AI can have on our society and the need to build trust, it is vital that European AI is grounded in our values and fundamental rights such as human dignity and privacy protection. Furthermore, the impact of AI systems should be considered not only from an individual perspective

That is why the Commission set out an AI strategy on 25 April 2018 addressing the socioeconomic aspects in parallel with an increase in investment in research, innovation and AI-capacity across the EU. It agreed a Coordinated Plan with the Member States to align strategies. The Commission also established a High-Level Expert Group that published Guidelines on trustworthy AI in April 2019.

.

The Commission published a Communication welcoming the seven key requirements identified in the Guidelines of the High-Level Expert Group:

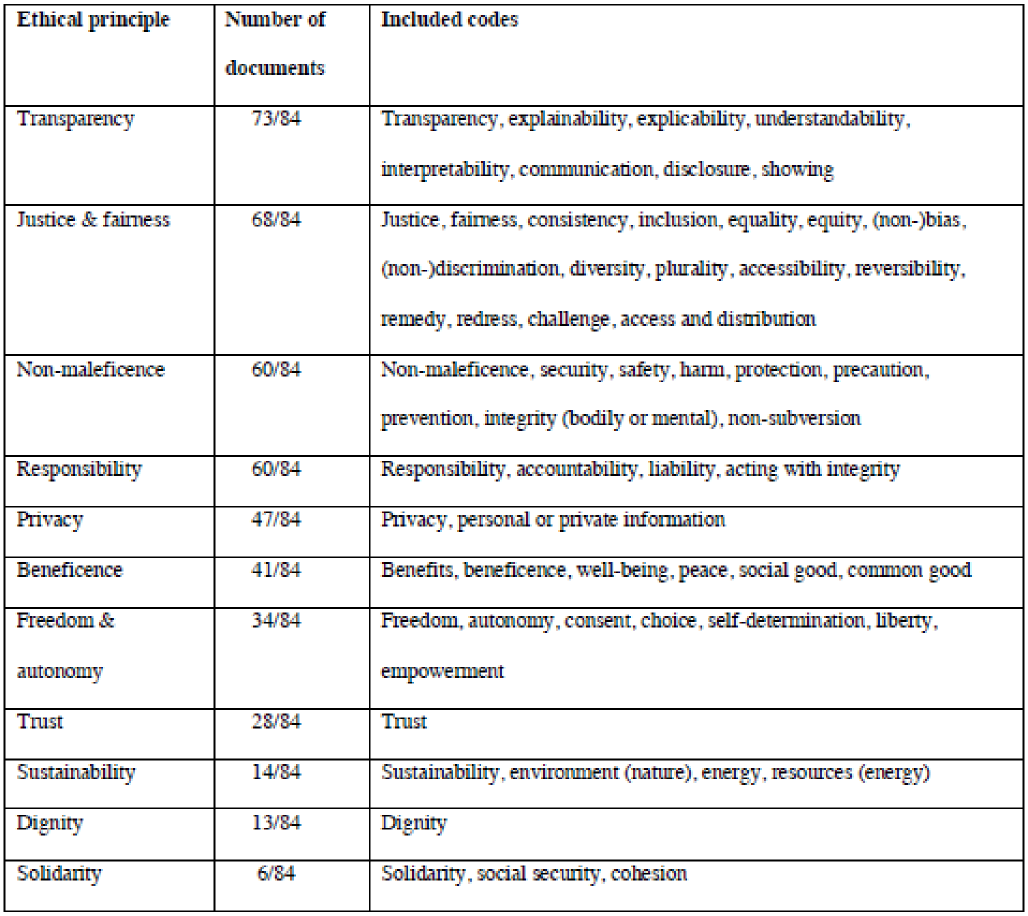
- Human agency and oversight,
- Technical robustness and safety,
- Privacy and data governance,
- Transparency,
- Diversity, non-discrimination and fairness,
- Societal and environmental wellbeing, and
- Accountability.

In addition, the Guidelines contain an assessment list for practical use by companies. During the second half of 2019, over 350 organisations have tested this assessment list and sent feedback. The High-Level Group is in the process of revising its guidelines in light of this feedback and will finalise this work by June 2020. A key result of the feedback process is that while a number of the requirements are already reflected in existing legal or regulatory regimes, those regarding transparency, traceability and human oversight are not specifically covered under current legislation in many economic sectors.

AI ETHICS GUIDELINES: A GLOBAL LITERATURE REVIEW

Jobin, Icena, Vayena, “AI: The Global Landscape of Ethics Guidelines” Health & Ethics Policy Lab, ETH Zurich, 2019.

To follow, a listing of those ethical principles most often cited in a 2019 review of 84 ethical use guidelines and frameworks:



Ethical principle	Number of documents	Included codes
Transparency	73/84	Transparency, explainability, explicability, understandability, interpretability, communication, disclosure, showing
Justice & fairness	68/84	Justice, fairness, consistency, inclusion, equality, equity, (non-)bias, (non-)discrimination, diversity, plurality, accessibility, reversibility, remedy, redress, challenge, access and distribution
Non-maleficence	60/84	Non-maleficence, security, safety, harm, protection, precaution, prevention, integrity (bodily or mental), non-subversion
Responsibility	60/84	Responsibility, accountability, liability, acting with integrity
Privacy	47/84	Privacy, personal or private information
Beneficence	41/84	Benefits, beneficence, well-being, peace, social good, common good
Freedom & autonomy	34/84	Freedom, autonomy, consent, choice, self-determination, liberty, empowerment
Trust	28/84	Trust
Sustainability	14/84	Sustainability, environment (nature), energy, resources (energy)
Dignity	13/84	Dignity
Solidarity	6/84	Solidarity, social security, cohesion

Although no single ethical principle is explicitly endorsed by all existing guidelines, transparency, justice and fairness, non-maleficence, responsibility and privacy are each referenced in more than half of all guidelines. This focus could be indicating a developing convergence on ethical AI around these principles in the global policy landscape. In particular, the prevalence of calls for transparency, justice and fairness points to an emerging moral priority to require transparent processes throughout the entire AI continuum (from transparency in the development and design of algorithms to transparent practices for AI use), and to caution the global community against the risk that AI might increase inequality if justice and fairness considerations are not adequately addressed.

IEEE: ETHICALLY ALIGNED DESIGN

https://ethicsinaction.ieee.org/

To strengthen individual agency, governments and organizations must test and implement technologies and policies that let individuals create, curate, and control their online agency as associated with their identity. Data transactions should be moderated and case-by-case authorization decisions from the individual as to who can process what personal data for what purpose.

Specifically, we recommend governments and organizations:

- **Create**: Provide every individual with the means to create and project their own terms and conditions regarding their personal data that can be read and agreed to at a machine-readable level.
- **Curate:** Provide every individual with a personal data or algorithmic agent which they curate to represent their terms and conditions in any real, digital, or virtual environment.
- **Control**: Provide every individual access to services allowing them to create a trusted identity to control the safe, specific, and finite exchange of their data. Three sections of this chapter reflect these core ideals regarding human agency

THE VATICAN: ROME CALL FOR AI ETHICS

The Vatican, 28 February 2020

http://www.academyforlife.va/content/dam/pav/documenti%20pdf/2020/CALL%2028%20febbraio/AI%20Rome%20Call%20x%20firma_DEF_DEF_.pdf

RIGHTS

The development of AI in the service of humankind and the planet must be reflected in regulations and principles that protect people – particularly the weak and the underprivileged – and natural environments. The ethical commitment of all the stakeholders involved is a crucial starting point; to make this future a reality, values, principles, and in some cases, legal regulations, are absolutely indispensable in order to support, structure and guide this process. To develop and implement AI systems that benefit humanity and the planet while acting as tools to build and maintain international peace, the development of AI must go hand in hand with robust digital security measures.

In order for AI to act as a tool for the good of humanity and the planet, we must put the topic of protecting human rights in the digital era at the heart of public debate. The time has come to question whether new forms of automation and algorithmic activity necessitate the development of stronger responsibilities. In particular, it will be essential to consider some form of "duty of explanation": we must think about making not only the decision-making criteria of AI-based algorithmic agents understandable, but also their purpose and objectives. These devices must be able to offer individuals information on the logic behind the algorithms used to make decisions. This will increase transparency, traceability and responsibility, making the computer-aided decision-making process more valid.

New forms of regulation must be encouraged to promote transparency and compliance with ethical principles, especially for advanced technologies that have a higher risk of impacting human rights, such as facial recognition.

To achieve these objectives, we must set out from the very beginning of each algorithm's development with an "algor-ethical" vision, i.e. an approach of ethics by design. Designing and planning AI systems that we can trust involves seeking a consensus among political decision-makers, UN system agencies and other intergovernmental organisations, researchers, the world of academia and representatives of non-governmental organizations regarding the ethical principles that should be built into these technologies. For this reason, the sponsors of the call express their desire to work together, in this context and at a national and international level, to promote "algor-ethics", namely the ethical use of AI as defined by the following principles:

1. ***Transparency****: in principle, AI systems must be explainable;*
2. ***Inclusion****: the needs of all human beings must be taken into consideration so that everyone can benefit and all individuals can be offered the best possible conditions to express themselves and develop;*
3. ***Responsibility****: those who design and deploy the use of AI must proceed with responsibility and transparency;*
4. ***Impartiality:*** *do not create or act according to bias, thus safeguarding fairness and human dignity;*
5. ***Reliability****: AI systems must be able to work reliably;*
6. ***Security and privacy:*** *AI systems must work securely and respect the privacy of users.*

##

2020.07.05