Human Systems Management 43 (2024) 591–604
DOI 10.3233/HSM-230099
IOS Press

Principles for facial recognition technology: A content analysis of ethical guidance in the United States

Heather Elaine Domin[a,*] and Sondria Miller[b]

[a]*Doctoral Program for Business Analytics and Data Science, Capitol Technology University, Laurel, MD, USA*
[b]*Doctoral Programs, Capitol Technology University, Laurel, MD, USA*

Received 2 June 2023
Accepted 3 November 2023

Abstract.
BACKGROUND: Facial recognition technology can significantly benefit society if used ethically. Various private sector, government, and civil society groups have created guidance documents to help guide the ethical use of this technology.
OBJECTIVE: The study's objective was to identify the common themes in these ethical guidance documents and determine the prevalence of those themes.
METHODS: A qualitative content analysis of 25 facial recognition technology ethical guidance documents published within the United States or by international groups that included representation from the United States.
RESULTS: The results show eight themes within the facial recognition technology ethical guidance documents: privacy, responsibility, accuracy and performance, accountability, transparency, lawful use, fairness, and purpose limitation. The most prevalent themes were privacy and responsibility.
CONCLUSIONS: By following common ethical recommendations, industry actors can help address the challenges that may arise when seeking to develop, deploy, and use facial recognition technology. The research findings can inform the current debates regarding the ethical use of this technology and might help further the development of ethical norms within the industry.

Keywords: Artificial intelligence, facial recognition technology, ethics, principles, content analysis

D r. Heather Domin is the Program Director for Tech Ethics by Design at IBM and Associate Director of the Notre Dame-IBM Tech Ethics Lab for IBM. She has a Ph.D. in Business Analytics and Data Science and is certified in agile and traditional project management methodologies (PMP, PMI-ACP, CSM).

D r. Miller is an acknowledged expert on STEM (Science, Technology, Engineering and Mathematics). She holds a Doctor of Psychology, a Master of Divinity, and a Bachelor of Science in Mathematics and provides logistics strategy for the Department of Defense Health Agency (DHA). She is also currently an Adjunct Professor at Capitol Technology University.

*Corresponding author: Heather Elaine Domin, Capitol Technology University, 11301 Springfield Rd, Laurel, MD 20708, USA. Tel.: +1 8669609620; E-mail: hedomin@captechu.edu.

1. Introduction

Widely effective and efficient across many different industries, the use of artificial intelligence (AI) and facial recognition technology (FRT) is growing at a rapid pace [1–3]. The AI software market size is expected to grow from less than 20 billion prior to 2020 to more than 120 billion by 2025 [3]. FRT adoption is also growing, with a global market size that is expected to reach 10 billion dollars by 2025 [2]. Adoption of these technologies has been influenced by vast amounts of online data and their utility in a variety of contexts, including those created by the Coronavirus Disease 2019 (COVID-19) [1, 2].

Global awareness of the COVID-19 pandemic occurred over the first few months of 2020, as it spread quickly across the world, leading governments to leverage intervention strategies to manage its impact such as lockdowns and other restrictions on in-person social interactions [4]. There was an increased fear of spreading the virus that causes this disease, which impacted global tourism [5]. The behaviors and attitudes of individuals changed as knowledge about the risks of the virus and social distancing practices became more common, driving increased use of online platforms and social media [6]. Factors such as changes in habits and technology awareness may have had a positive effect on the shift toward the adoption of this technology, for example, to support online shopping activities [7]. An effect of these responses by organizations and individuals to addresses the COVID-19 was a growing amount of online data, including facial data, and increasing demand for AI and FRT for purposes such as security and attendance tracking [1, 2].

While ethical issues can be found in other types of technology systems, the potential scale of impact and the rapid rate at which AI and FRT are being adopted are key factors in driving widespread concern [8, 9]. FRT has been a significant area of focus given the widely acknowledged challenges this technology can introduce around individual privacy and fair outcomes for minority groups [10, 11–14]. Evidence of problematic use of this technology, including wrongful arrests and surveillance in public areas, has helped fuel this focus [10, 14, 15]. Despite the growing awareness of potential ethical issues associated with FRT, the extent to which ethical principles for the use of this technology are converging, is not yet fully explored. While comprehensive research on AI ethics principles does exist, this study aims to help fill the specific gap in research on principles for FRT [16–19].

2. Artificial intelligence, facial recognition technology, and ethics

2.1. Defining artificial intelligence and facial recognition technology

There is currently no common consensus on how to define AI, and while some definitions focus on popular technical approaches such as machine learning and the methods by which they are developed, many are broad [20, 21]. At the broadest possible understanding of the term, AI is the ability of a machine to mimic a human's behavior or capability [21–23].

FRT typically refers to systems that use facial images for the purpose of person identification or verification; however, much of the same core technology can also be used to detect a face (without necessarily relating it back to an individual) or to extract information from facial images such as emotional expression [13, 24, 25]. The capabilities are interrelated because it is typically necessary to perform the first phases of detecting a face and relevant features from an image before performing tasks such as facial analysis [24, 26]. While there is a valid argument that more simplistic FRT systems are not AI systems, under the broadest definition of AI, even simplistic methods could be considered as replicating a human's ability to recognize an individual or attributes of a person's face. However, this debate is mostly irrelevant now because while early FRT methods were simplistic in nature, many modern FRT systems leverage widely agreed AI techniques such as convolutional neural networks [22, 24, 27].

2.2. Ethical issues and potential solutions

Ethical issues in AI and FRT are overlapping, which is not surprising given the close relationship in how these technology areas are defined. While the potential ethical issues in these technology areas can drive significant attention, the adoption of these technologies would not be occurring at such a rapid rate if they were not also providing significant benefits. Some of these benefits of AI and FRT include the potential usefulness, efficiency, sustainability, safety, impartiality, non-intrusiveness, cost savings, and economic opportunity associated with these systems [24, 28–30]. AI and FRT technologies were beneficial

during the COVID-19 pandemic, but also fueled an environment where ethical considerations are critical [1, 2]. The counter measures taken by governments to limit the spread of the disease had a significant influence on the daily habits of individuals, including on dietary habits and the diversity of foods that individuals consumed [31]. Organizations also had to adapt to the COVID-19 pandemic. For example, many academic institutions and their student populations embraced online library services as social norms and attitudes changed [32]. Many private sector organizations adapted to the new realities of COVID-19 by adjusting their strategies and increasing innovation to survive during a period of supply chain disruption and increased competition within the marketplace [33]. Some businesses benefited from this new reality. For example, increased competition has had a positive effect on financial performance measures of businesses in China [5]. However, increased online activity and the associated data can fuel ethical concerns.

2.2.1. Ethical issues associated with AI

Artificial intelligence ethical issues that are commonly acknowledged include the potential for privacy invasion, unfair outcomes, lack of responsible actions, limited accountability, the potential for misaligned goals, and inadequate transparency [8, 9, 16–18]. Examples of ethical issues that have occurred in recent years include biased performance in a criminal recidivism prediction algorithm, the racially offensive output produced by a chatbot trained on social media data, the perpetuation of gender stereotypes in a chatbot, and politically influential content prioritization in social media platforms [8, 9]. The ethical issues associated with AI and the potential solutions have been explored by a variety of academic, government, and civil society groups [8, 9, 16–18].

2.2.2. Ethical issues associated with facial recognition technology

Ethical issues have also occurred in the use of FRT, fueling an international focus on potential ethical issues such as potential privacy violations and biased performance between demographic groups [10–13, 34–36]. These ethical issues are particularly concerning in the context of law enforcement because misidentification can result in the potential loss of civil liberties [15, 35, 37, 38]. Documented cases such as the 2020 wrongful arrest of Robert Williams in Detroit, the use of FRT on individuals gathering after the death of George Floyd in 2020, and on individuals at the U.S. Capitol in 2021 highlight the need to remain vigilant about protecting against these potential issues [14, 15].

Biased performance in FRT has been a documented issue within research literature since the early 1990s [39]. Despite the evidence of this issue, Garvie et al. [37] found that testing for bias was not common among law enforcement organizations. A study by Buolamwini and Gebru [40] brought attention to the issue of bias in tools capable of facial recognition when they demonstrated large accuracy differentials based on gender and skin tone for the task of gender classification. Another report that drew significant attention to the potential for biased performance was conducted by researchers at the National Institute of Standards and Technology [12], who found in their assessment of 189 algorithms that bias across demographic groups can be an issue for facial recognition identification and verification tasks.

2.2.3. Principles and potential solutions

In response to growing awareness of the potential ethical issues associated with AI and FRT, governments and other organizations have published guidance relating to ethical principles [16–19]. Algorithm Watch's "AI Ethics Guidelines Global Inventory" includes 167 such guidelines [41]. Jobin et al. [18 p391] studied 84 AI ethics guidelines from around the world and found common principles to be "transparency, justice and fairness, non-maleficence, responsibility and privacy." Fjeld et al. [16 p67] also mapped principles across a set of 36 documents containing AI principles and found themes that included "Privacy, Accountability, Safety and Security, Transparency and Explainability, Fairness and Non-discrimination, Human Control of Technology, Professional Responsibility, and Promotion of Human Values."

While the themes in general AI guidelines have been studied and potential solutions explored by various researchers and groups, to the best of our knowledge, there is no comprehensive research on the themes within FRT ethical guidelines. Several AI ethics guidance researchers have noted the need for future research on more focused AI ethics guidelines and the value of finding common themes [16–19]. Thus, the objective of this study is to help fill this gap in the literature and inform the ongoing debates regarding the ethical use of FRT.

3. Paper objective and research purpose

This paper will describe a qualitative content analysis study conducted on 25 ethical guidance documents for FRT. The purpose of the study was to identify the common themes in these ethical guidance documents and determine the prevalence of these themes. The objective of the paper is to convey the study's methodology and research findings so that they can be used by a variety of stakeholders in the context of future research, policy, and industry deployments of FRT.

4. Research design and data collection

A qualitative content analysis research methodology with an inductive research design was selected for this study because it best supported the research objectives. Content analysis involves extracting themes directly from documents or other media [42].

Document collection was achieved using a systematic procedure based upon the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework [43] adapted by Jobin et al. [18] for their study on AI ethics guidance documents. Systematic analysis of pre-existing data sets is a useful method for many research areas, for example, pre-existing data on human diseases can be used to help assess the effectiveness of a nation's health care system [44]. The PRISMA framework can therefore be applied to a variety of subject areas, and the adapted version from Jobin et al. [18] provided the necessary categorical structure for the identification of FRT documents relevant to this study.

Documents were identified through a variety of internet-based search portals and then supplemented with citation chaining to identify additional documents not found through the internet-based search. The internet-based portals included Algorithm Watch's "AI Ethics Guidelines Global Inventory" [41] linkhub website, Google, Microsoft Bing, and Capitol Technology University's virtual library. The search terms included *facial recognition technology ethical guidance, facial recognition ethical guidance, facial recognition technology ethical guidelines, facial recognition ethical guidelines, facial recognition technology guardrails, facial recognition guardrails, facial recognition technology principles, facial recognition principles, facial recognition technology ethics, and facial recognition ethics*. Adhering to the adapted PRISMA procedure, the first 30 search results for each of the search terms were evaluated fully to assess if the results met the criteria for inclusion. The search results up to the 200th link were also screened, but only for the primary search term (facial recognition technology ethical guidance). Figure 1 shows the document collection procedure and the number of documents identified through a linkhub, web search, and citation chaining.

Documents were selected using a purposive sampling method, a method that enables the identification of documents that were most relevant to the purpose of the study and the research questions [45]. The inclusion criteria were that the document be normative in nature, accessible via the internet through the internet-based search portals available, grey literature that was published by a civil society, government, or private sector organization, published within the United States or by an international organization that included members from the United States, and published between January 2016 and June 2021. Duplicates were excluded. The United States was targeted as a geographic region given its large market share in the global FRT market and that it is home to many large technology companies developing this technology [2]. The United States also has a history of systemic racism driving many of the ethical concerns and therefore provides a useful microcosm for study [36]. A total of 25 documents were identified for inclusion in this study, 11 from civil society, 5 from government, and 9 from private sector organizations. Table 1 provides a list of the documents.

Following document collection, the documents were analyzed for common recommendations, which, at the highest categorical level, represent principles for FRT. The qualitative content analysis process involved the three phases of preparation, organization, and resulting [42]. Coding was completed manually in digital copies of the documents using NVivo software. Given the inductive research design, the lowest level recommendations were coded first, and then these codes were gradually abstracted to subcategories and the higher-order themes and ethical principle categories. The coded data was used to calculate descriptive statistics regarding the frequency with which these themes occurred within the documents. Descriptive statistics on frequency are useful for reporting results in a variety of contexts; for example, descriptive statistics have been used to help answer research questions about the health needs of boys aged 10–15 in Iran [46]. Similar approaches to reporting results have also been used in prior studies on general AI ethics principle documents [16–19].

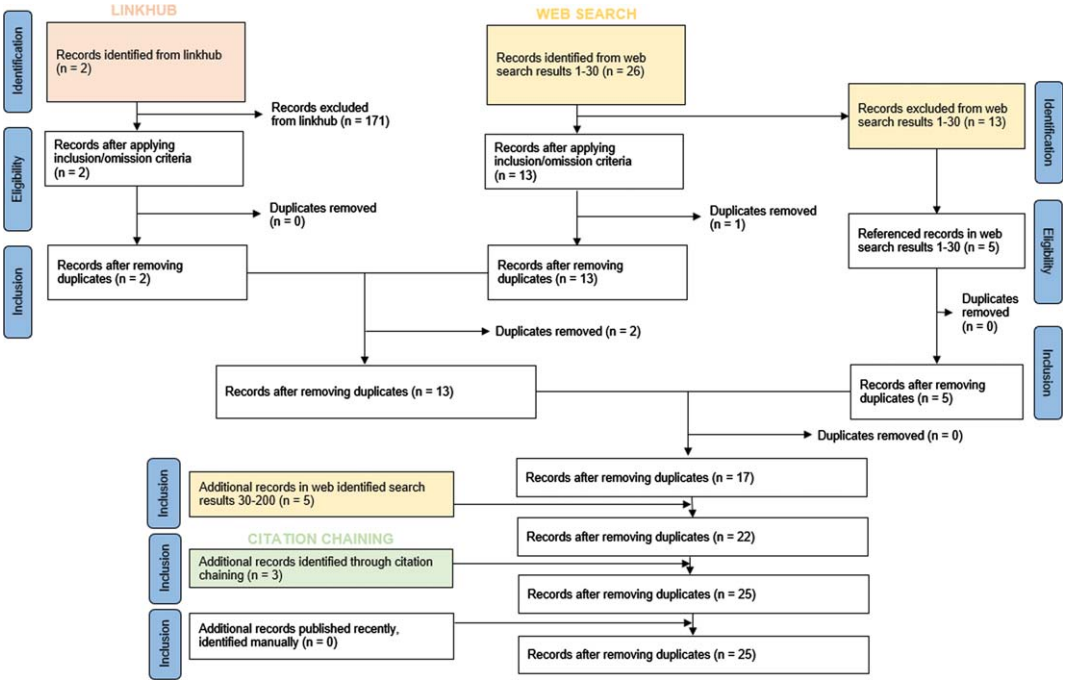

Fig. 1. Results of the document collection procedure using an adapted Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework. Adapted from Jobin et al. (2019). Copyright 2019 by Springer Nature Ltd.

5. Results: Themes

The common recommendations identified from the 25 documents included in this study represent the views of powerful industry actors from a variety of civil society, government, and private sector groups. Collectively, the themes in common recommendations from these groups form a basis for ethical principles for FRT. Common themes across documents included privacy, responsibility, accuracy and performance, accountability, transparency, lawful use, fairness, and purpose limitation. Figure 2 contains a view of the final thematic categories and subcategories. Some of these themes were more prevalent than others; the most frequent recommendations within the documents were for privacy, responsibility, and accuracy and performance. Differences among the recommendations from the organizational groups were also observed. Table 2 shows the number and percentage of documents that contained each thematic category by organization type.

5.1. Privacy

Privacy is considered a universal human right, and organizations frequently highlight the notion that FRT should not infringe upon this right [47]. The theme of privacy was, in fact, identified in 100% of the documents and was, therefore, amongst the most prevalent themes identified. A common recommendation was that privacy should be protected and data should be secured, especially in high-risk contexts where there is a reasonable expectation of individual privacy. Documents often pointed to the United States Constitution's Fourth Amendment; for example, Geraghty [48 p14] stated in the National League of Cities (NLC) document that "the Fourth Amendment protects people from unlawful police searches where they have a reasonable expectation of privacy." The documents also highlighted how privacy remains a focus despite potentially competing priorities; for example, SAFR [49 para1] stated that while education leaders are concerned about safety, they are also "equally vigilant about protecting the privacy of staff, students, and visitors at the schools."

5.2. Responsibility

Recommendations relating to the concept of responsibility were identified in 100% of the documents. A common recommendation was that organizations take steps to ensure both the respon-

Table 1
List of facial recognition technology ethical guidance documents

Document	Organizational Group	Source
	Civil Society	
1. 10 Actions that Will Protect People from Facial Recognition Software	Brookings	Web search
2. A Framework for Responsible Limits on Facial Recognition Use Case	World Economic Forum (WEF)	Linkhub
3. Facial Recognition Policy Principles	U.S. Chamber of Commerce, Chamber Technology Engagement Center (C_TEC)	Web search
4. Facial Recognition Report	National League of Cities (NLC)	Web search
5. First Report of the Axon AI Ethics Board: Face Recognition	Axon AI Ethics Board, facilitated by the Policing Project at NYU School of Law	Web search
6. Guiding Principles for Law Enforcement's Use of Facial Recognition Technology	Integrated Justice Information Systems Institute (IJIS) Institute and the International Association of Chiefs of Police (IACP), Law Enforcement Imaging Technology Task Force (LEITTF)	Web search
7. Privacy Principles for Facial Recognition Technology in Commercial Applications	Future of Privacy Forum (FPF)	Web search
8. Safe Face Pledge	Algorithmic Justice League and the Center on Privacy & Technology at Georgetown Law, Safe Face Pledge	Web search
9. SIA Principles for the Responsible and Effective Use of Facial Recognition Technology	Security Industry Association (SIA)	Web search
10. Statement of Principles on Facial Recognition Policy	American Legislative Exchange Council (ALEC)	Web search
11. Statement on Principles and Prerequisites for the Development, Evaluation, and Use of Unbiased Facial Recognition Technologies	Association for Computing Machinery (ACM), U.S. Technology Policy Committee (USTPC)	Web search
	Government	
12. Face Recognition Policy Development Template	U.S. Department of Justice, Bureau of Justice Assistance (BJA)	Citation chaining
13. Facial Identification Practitioner Code of Ethics	Facial Identification Scientific Working Group (FISWG)	Citation chaining
14. Facial Recognition Technology: Ensuring Transparency in Government Use	Federal Bureau of Investigation (FBI)	Citation chaining
15. Facial Recognition Technology Privacy and Accuracy Issues Related to Commercial Uses	United States Government Accountability Office (U.S. GAO)	Web search
16. Privacy Best Practice Recommendations for Commercial Facial Recognition Use	National Telecommunications and Information Administration (NTIA)	Web search
	Private Sector	
17. Can Facial Recognition Technology Be Used Ethically?	ImageWare	Web search
18. How to Use Facial Recognition Technology Responsibly and Ethically	Gartner	Web search
19. Key Considerations for the Ethical Use of Facial Recognition Technology	Avanade	Web search
20. Our Approach to Facial Recognition	Google	Web search

(*Continued*)

Table 1
(*Continued*)

Document	Organizational Group	Source
21. Precision Regulation and Facial Recognition	IBM	Web search
22. Privacy by Design: Best Practices for Using Facial Recognition to Support Safer K-12 Campuses	SAFR	Web search
23. Six Principles for Developing and Deploying Facial Recognition Technology	Microsoft	Web search
24. Some Thoughts on Facial Recognition Legislation	Amazon Web Services (AWS)	Web search
25. Why We've Never Offered Facial Recognition	Salesforce	Web search

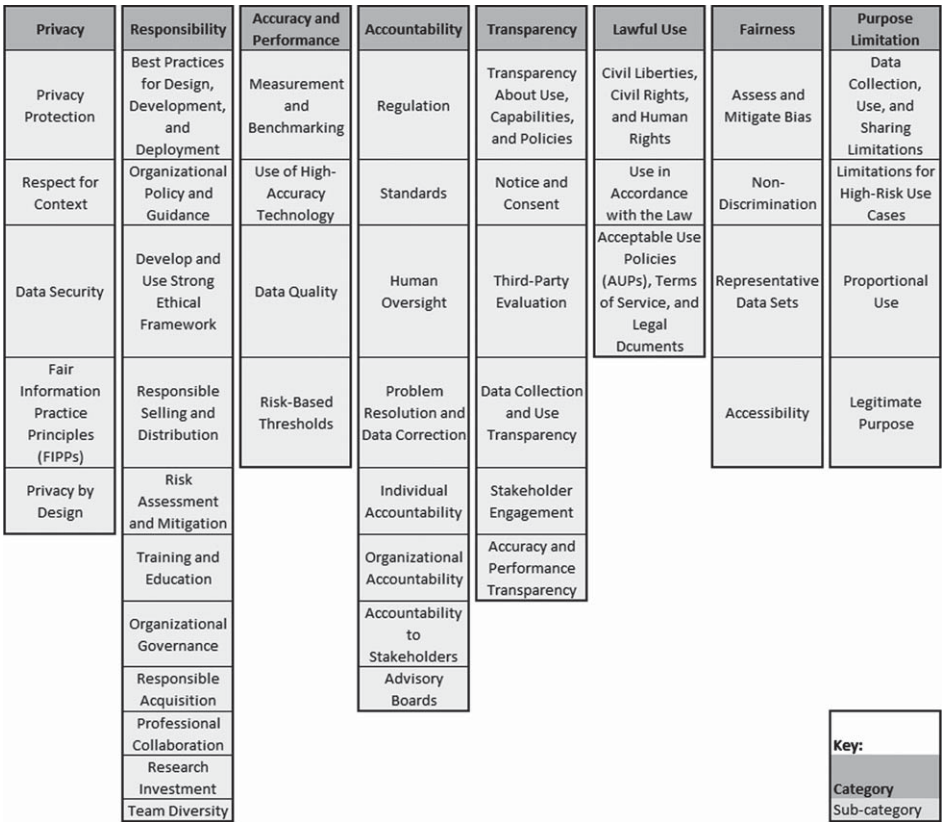

Fig. 2. Final thematic categories and subcategories.

sible creation and implementation of FRT. For example, the United States Chamber of Commerce Chamber Technology Engagement Center [50 p1] highlighted businesses "have a responsibility to ensure the safe development and deployment of facial recognition technology." The documents also highlighted that responsibility extends beyond the scope of the technology system itself and must also factor in broader organizational policy and guidance. For example, the Integrated Justice Information Systems Institute and the International Association of Chiefs of Police and Law Enforcement Imaging Technology Task Force [51] recommended required training before using the technology in a law enforcement context. Further, FBI director Kimberly J. Del Greco testified that agencies should "ensure that comprehensive policies are developed, adopted, and implemented in order to guide the entity and its personnel in the day-to-day access and use of facial recognition technology" [52 para25].

5.3. Accuracy and performance

Accuracy and performance recommendations within the documents frequently related to measuring and enabling these aspects in FRT, including ensuring adequate quality in associated data. The accuracy and performance theme was identified in 92% of the documents. It is likely that many of these recommendations were influenced by NIST's "Face recognition vendor test (FRVT) Part 3: Demographic effects" report which called attention to the fact that there can be a reduced risk of differences in error rates across demographic groups when algorithms with the highest overall accuracy rates are used [12, 53]. The United States Government Accountability Office [13] document had "accuracy" in its title and, in addition to privacy, was a primary theme within that document. World Economic Forum [54 p9] puts a heavy focus on performance, highlighting it as a key principle and recommending that organizations evaluate the "accuracy and performance of their systems at the design (lab tests) and deployment (field tests) stages." West [55 para12] recommended in the Brookings document that there be mandated standards relating to accuracy but acknowledged that it could be a challenge to "determine how high accuracy levels should be before FR is deployed in a widespread basis." Achieving maximum levels of accuracy and performance can be challenging, given that it is not just one-time consideration. Greene [53 para24] pointed out in the ImageWare document that algorithms will need to be upgraded "as new and improved algorithms are developed (which is constant!)."

5.4. Accountability

Accountability was a theme found in 88% of the documents. These documents commonly referenced a need for accountability mechanisms to help ensure the responsible creation and implementation of FRT. For example, the Future of Privacy Forum (FPF) included accountability as one of the core principles within their document, noting that it may involve parties outside of the organization itself when recommending "reasonable steps to ensure that the use of facial recognition technology and data by the organization, and in partnership with all third-party service providers or business partners, adheres to these principles" [57 p11]. Accountability also appeared as a strong theme in organizations that drew from the existing FIPPs framework, which is not surprising given that the FIPPs include accountability as a core principle [13, 57–59]. The documents highlighted the importance of regulation in enabling accountability; however, it was also clear that there are several other types of accountability mechanisms that organizations should also be considered. For example, Facial Identification Scientific Working Group [59 p1] recommended that individuals who violate their ethical principles for facial identification practitioners "be reported to the FISWG executive board." Individual accountability can be important for "developers, operators, and users" of FRT systems [60 p4].

5.5. Transparency

Recommendations for transparency, found in 84% of the documents, often focused on the importance of being transparent both about the use and capabilities of FRT systems. For example, Algorithmic Justice League and Center on Technology and Privacy at Georgetown Law [61] included the facilitation of transparency as one of the four primary organizational commitments outlined within the document. Transparency also appeared as a major category of recommendations within the American Legislative Exchange Council [62], Future of Privacy Forum [56], United States Department of Commerce National Telecommunications and Information Administration [63], SAFR [49], and Security Industry Association [58] documents. The American Legislative Exchange Council [62 para20] highlighted how transparency is fundamental, with the declaration that "transparency is the bedrock that governs the use of facial recognition technology." Examples of recommended transparency practices included making "available to consumers, in a reasonable manner and location, policies or disclosures" [63 p1], documenting and communicating "the capabilities and limitations of facial recognition technology" [64 p1], and making performance assessments "auditable by competent third-party organizations and their reports made available to users of the systems" [64 p9].

5.6. Lawful use

Taking steps to ensure the lawful use of FRT was a common recommendation within the documents, a theme found within 84% of the documents. For instance, Microsoft Corporation [63 p3] named "lawful surveillance" as a core principle for FRT. World Economic Forum [53 p8] included a pointed recommendation that organizations who attempt to pilot

Table 2
Frequency of thematic categories by organization type

	Civil Society		Government		Private Sector		Total	
Category	No.	%	No.	%	No.	%	No.	%
Privacy	11	100%	5	100%	9	100%	25	100%
Responsibility	11	100%	5	100%	9	100%	25	100%
Accuracy and Performance	10	91%	5	100%	8	89%	23	92%
Accountability	11	100%	5	100%	6	67%	22	88%
Transparency	10	91%	4	80%	7	78%	21	84%
Lawful Use	10	91%	3	60%	8	89%	21	84%
Fairness	10	91%	2	40%	8	89%	20	80%
Purpose Limitation	10	91%	4	80%	4	44%	18	72%
Total	11	100%	5	100%	9	100%	25	100%

their principles "be lawful." Similarly, American Legislative Exchange Council [62 para3] recommended that "policymakers should ensure that government entities, especially law enforcement, only use facial recognition for legitimate, lawful and well-defined purposes." The general calls for lawful use were frequently tied to concerns over the possible infringement of basic human liberties and rights, and the specific recommendations for ensuring appropriate policies, terms, and legal documentation were aimed at reducing the risk of unlawful use.

5.7. Fairness

Fairness recommendations, found within 80% of the documents, commonly highlighted that organizations should take appropriate steps to enable fairness when creating and implementing FRT. A typical sentiment can be found in Google's statement that FRT "needs to be fair, so it doesn't reinforce or amplify existing biases, especially where this might impact underrepresented groups" [65 para4]. A similar sentiment can be found in the Avanade document, which highlighted the importance of ensuring FRT be "fair and inclusive" [68 para4]. The documents frequently identified the risk of unfairness as a key concern, often driven by underlying issues such as a lack of representative data sets used by FRT systems [13, 48, 54–56, 60, 61, 66–69]. Taking steps to ensure fairness is particularly important in high-risk contexts such as law enforcement, and as Goldman [70 para4] warned within the Salesforce document, "the use of facial recognition in public spaces can create opportunities for political manipulation, discrimination, and more" and that the "risks to transgender, nonbinary, or gender non-conforming individuals are also acute."

5.8. Purpose limitation

Purpose limitation of both the FRT system and associated data were common recommendations within the documents, a theme identified within 72% of the documents. The potential risk and expectations of stakeholders were highlighted as key considerations when determining how the purpose of the system and data should be limited. These considerations clearly draw from data privacy concepts on purpose limitation but expand upon this concept to also consider how the system's use case should be limited. The relationship between the data and the system's use case is inextricably tied, given that expanding the use case beyond how it was originally intended to be used may also result in data that is used beyond its originally intended purpose or may even result in new data.

As stated by Geraghty [48 p33] in the NLC document, in the context of law enforcement, there should be limits on the "scope of facial recognition use to reduce the risk of misidentifications and privacy violations." Montgomery and Hagemann [64 p2] also highlighted certain use cases as a concern within the IBM document, where it was stated that there are some "clear use cases that must be off-limits" and "mass surveillance" and "racial profiling" were offered as examples. Similar sentiments were echoed in other documents as well, which highlighted the importance of requiring limitations in the use of FRT in surveillance contexts and in body-worn camera use cases [48, 55, 66, 68]. Within the Gartner document, Sakpal [71 para8] pointed out the importance of ethical proportionality in the context of facial recommendation technology, "it means that an organization should use technology powerful enough

to solve a particular problem, but not much more powerful."

6. Discussion and interpretations

6.1. Comparison by organizational type

A comparison between the ethical recommendations made by private sector, government, and civil society organizations also revealed some uniqueness. Differences are likely due to multiple factors, including diversity. Documents from private sector organizations contained fewer recommendations for transparency (78% of documents), accountability (67%), and purpose limitation (44%) compared to government and civil society groups. Documents from government organizations had fewer recommendations for lawful use (60%) and fairness (40%). Documents from civil society groups had greater than 90% of documents that contained recommendations from each of the themes identified in this study. A review of the members who participate in the civil society groups reveals that these groups tend to have a great deal of diversity. This diversity in membership may contribute to the consistency across all recommendation categories, given the breadth of perspectives that contributed to them.

6.2. Discussion on the impact of COVID-19

The COVID-19 pandemic created scenarios where increased focus on FRT ethics is needed, given its impact on the global supply chain and organizations across many industries [72]. For example, in the COVID-19 context, online social media platforms have helped organizations disseminate information; therefore, increased use of these platforms can be beneficial [73]. However, it is ethical, and possibly legally required, to limit the use of the facial image data created in online social media platforms to their intended purpose. Furthermore, in this context it is ethical to deploy systems that are accurate and perform well for their task, as well as to offer alternatives that do not require the use of face data. For example, screening potential COVID-19 patients over the telephone [74].

7. Limitations and conclusions

7.1. Limitations

This study is not without limitations. The timeframe for data collection of guidance documents was limited to documents produced between January 2016 and June 2021, and additional guidance documents that might meet the inclusion criteria published after June 2021 were not included. Documents that were produced outside of the geographic scope were also not included, and this could impact the generalizability of the findings. Documents as data sources also have the potential to be incomplete or inaccurate [75]. Finally, researcher bias is possible where the researcher is the primary instrument for data collection [75–77]. Steps to mitigate these limitations were addressed through documentation of procedures, triangulating against multiple data sources, and involving subject matter experts for review [75, 77–80]. However, future research is required to fully address these limitations and confirm the generalizability of the findings.

7.2. Concluding remarks and future directions

Using a qualitative content analysis research methodology, eight common themes were identified across 25 documents produced by government, private sector, and civil society organizations. The resulting themes, which are also principles for FRT, include privacy, responsibility, accuracy and performance, accountability, transparency, lawful use, fairness, and purpose limitation. This study is significant because it helps fill a current gap in the body of knowledge on themes in ethical guidance documents for FRT, presenting a novel view of the convergent principles to which they are aligned. The results can be leveraged by organizations. For example, if an organization identifies a need to increase their focus on transparency, they may choose to adopt practices identified in subcategory themes such as sharing information on the organization's use of FRT and current policies and engaging with stakeholders to gather feedback. The results may also help inform policymakers as they develop policies and regulations, those developing industry standards, and other stakeholders within the industry who are looking to help develop common ethical norms that support the best interest of society. For example, policymakers who aim to regulate FRT such that citizens are maximally protected from potential harm can review draft regulations against the results of this study to confirm that common recommendations are fully addressed. Other stakeholders, such as those from industry associations or advocacy groups, may also find the results of this study inform their understanding of existing common recommendations and how their views may

relate to those of other organizations, which can help them develop a robust point of view.

Future research on FRT ethical guidance documents produced by organizations in other geographic regions of the world and at the global level would be beneficial. Given the differences observed in recommendations between government, private sector, and civil society groups, it would also be useful to explore why these differences occur and the implications of the root causes. Evaluating how these principles are implemented within organizations would also be useful to identify their effectiveness in practice. This evaluation could help determine if and how the principles guide FRT's ethical development, deployment, and use. For example, a study focused on notice and consent practices could help determine their effectiveness when used by organizations to help put the transparency principle into practice. It could also lead to identifying strategies that can improve their effectiveness in achieving the desired level of transparency. Research investment was found to be a subcategory theme within the ethical guidance documents studied, and the researchers involved in this study echo this call for prioritizing research that helps enable alignment with ethical principles for FRT systems.

Acknowledgments

The study is also documented in: Domin H (2022) Principles for Facial Recognition Technology: A Content Analysis of Ethical Guidance. Dissertation, Capitol Technology University. Approval was obtained from Capitol Technology University's Institutional Review Board.

Author contributions

Author 1 conceptualized the study, designed the methodology, performed data collection and analysis, wrote the manuscript, and performed revisions under the supervision of Author 2. Author 2 provided feedback and guidance on the concept, methodology, data, manuscript. revisions, and provided supervision to Author 1.

References

[1] Modor Intelligence. Facial recognition market – growth, trends, and forecasts (2020–2025). Hyderabad; 2019.

[2] Research and Markets. Global facial recognition market forecast from 2019 up to 2025 (Description). Dublin; 2019.

[3] Statistica. Global AI software market size 2018–2025 [Internet]. Available from: https://www.statista.com/statistics/607716/worldwide-artificial-intelligence-market-revenues. [Accessed 21 May 2023].

[4] Zhou Y, Draghici A, Mubeen R, Boatca ME, Salam MA. Social media efficacy in crisis management: effectiveness of non-pharmaceutical interventions to manage COVID-19 challenges. Frontiers in Psychology [Internet]. 2022;12(1099):626134. DOI:10.3389/fpsyt.2021.626134

[5] Li X, Dongling W, Baig NUA, Zhang R. From cultural tourism to social entrepreneurship: Role of social value creation for environmental sustainability. Frontiers in Psychology [Internet]. 2022;13. DOI: 10.3389/fpsyg.2022.925768

[6] Yu S, Draghici A, Negulescu OH, Ain NU. Social media application as a new paradigm for business communication: The role of COVID-19 knowledge, social distancing, and preventive attitudes. Frontiers in Psychology [Internet]. 2022;13. DOI: 10.3389/fpsyg.2022.903082

[7] Al Halbusi H, Al-Sulaiti K, Al-Sulaiti I. Assessing factors influencing technology adoption for online purchasing amid COVID-19 in Qatar: Moderating role of word of mouth. Frontiers in Environmental Science [Internet]. 2022;13:942527. DOI: 10.3389/fenvs.2022.942527

[8] Coeckelbergh M. AI Ethics. London, England: MIT Press; 2020.

[9] Wooldridge M. A brief history of artificial intelligence: What it is, where we are, and where we are going. Flatiron Books; 2021.

[10] Fitch A. Amazon suspends police use of its facial-recognition technology. Wall Street Journal (Eastern ed) [Internet]. 2020 Jun 10. Available from: https://www.wsj.com/articles/amazon-suspends-police-use-of-its-facial-recognition-technology-11591826559. [Accessed 16 July 2020].

[11] Congressional Digest. Legislative background on facial recognition: is Congress ready to ban biometric technology? Congressional Digest; 2020;99:16-17.

[12] National Institute of Standards and Technology. Face recognition vendor test (FRVT) part 3: demographic effects, NIST Publication No. IR 8280 [Internet]. Gaithersburg (MD); 2019.

[13] United States Government Accountability Office. Facial recognition technology: privacy and accuracy issues related to commercial uses, GAO Publication No. 20-522. Washington (DC); 2020.

[14] United States Government Accountability Office. Facial Recognition Technology: federal law enforcement agencies should better assess privacy and other risks, GAO Publication No. 21-518. Washington (DC); 2021.

[15] Ho D, Black E, Agrawala M, Fei-Fei L. Evaluating facial recognition technology: A protocol for performance assessment in new domains [Internet]. Stanford.edu. Available from: https://hai.stanford.edu/sites/default/files/2020-11/HAI_FacialRecognitionWhitePaper.pdf. [Accessed 20 Novemer 2022].

[16] Fjeld J, Achten N, Hilligoss H, Nagy A, Srikumar M. Principled artificial intelligence: Mapping consensus in ethical and rights-based approaches to principles for AI. SSRN Electron J [Internet]. 2020. DOI: 10.2139/ssrn.3518482

[17] Hagendorff T. The ethics of AI ethics: An evaluation of guidelines. Minds Mach (Dordr) [Internet]. 2020;30(1):99-120. DOI: 10.1007/s11023-020-09517-8

[18] Jobin A, Ienca M, Vayena E. The global landscape of AI ethics guidelines. Nat Mach Intell [Internet]. 2019;1(9):389-99. DOI: 10.1038/s42256-019-0088-2

[19] Zeng Y, Lu E, Huangfu C. Linking artificial intelligence principles. In: Espinoza H, hÉigeartaigh SO, Huang X, Hernández-Orallo J, Castillo-Effen M (eds) Proceedings of the AAAI workshop on artificial intelligence safety 2019. CEUR Workshop Proceedings; 2018:1-4. arXiv:1812.04814. 2019.

[20] Mccarthy J. What is artificial intelligence? [Internet]. 2007. Stanford.edu. Available from: http://jmc.stanford.edu/articles/whatisai/whatisai.pdf. [Accessed 21 May 2023].

[21] Samoili S, Cobo ML, Gómez E, De Prato G, Martínez-Plumed F, Delipetrev B. AI watch defining artificial intelligence: towards an operational definition and taxonomy of artificial intelligence. European Commission Joint Research Center, Ispra; 2020.

[22] Leong B, Jordan S. The spectrum of artificial intelligence: companion to the FPF AI infographic. Future of Privacy Forum. 2021. Available from: https://fpf.org/wp-content/uploads/2021/08/FPF-AIEcosystem-Report-FINAL-Digital.pdf. [Accessed 14 April 2022].

[23] Saravanan MK, Department of MBA Sree Vidyanikethan Inst., of Management Tirupati, Andhra Pradesh, India. A review of artificial intelligence systems. Int J Adv Res Comput Sci [Internet]. 2017;8(9):418-21. DOI: 10.26483/ijarcs.v8i9.5095

[24] Adjabi I, Ouahabi A, Benzaoui A, Taleb-Ahmed A. Past, present, and future of face recognition: A review. Electronics (Basel) [Internet]. 2020;9(8):1188. DOI: 10.3390/electronics9081188

[25] Ullah EAI, Khanum MA. A comparative study of facial recognition systems. Int J Adv Res Comput Sci. [Internet]. 2018;9:114-7. DOI: 10.26483/ijarcs.v9i0.6148

[26] Raji I, Fried G. About face: a survey of facial recognition evaluation. arXiv:210200813. 2021.

[27] Wang M, Deng W. Deep face recognition: A survey. Neurocomputing. 2021;429:215-44. DOI: 10.1016/j.neucom.2020.10.081

[28] European Commission. White paper on artificial intelligence: a European approach to excellence and trust. Brussels: 2020.

[29] Ryan M, Antoniou J, Brooks L, Jiya T, Macnish K, Stahl B. Technofixing the future: ethical side effects of using AI and big data to meet the SDGs. In: Proceedings of IEEE smart world Congress 2019. IEEE, Leicester, UK; 335-341. DOI: 10.1109/SmartWorld-UIC-ATC-SCALCOM-IOP-SCI.2019.00101

[30] Maxim M, Pikulik E. Cambridge: Navigating the Emerging Risks of Biometric Technologies; 2020.

[31] Geng J, Ul Haq S, Ye H, Shahbaz P, Abbas A, Cai Y. Survival in pandemic times: Managing energy efficiency, food diversity, and sustainable practices of nutrient intake amid COVID-19 crisis. Frontiers in Environmental Science [Internet]. 2022;13:945774. DOI: 10.3389/fenvs.2022.945774

[32] Rahmat TE, Raza S, Zahid H, Mohd Sobri F, Sidiki S. Nexus between integrating technology readiness 2.0 index and students' e-library services adoption amid the COVID-19 challenges: Implications based on the theory of planned behavior. J Educ Health Promot [Internet]. 2022;11(1):50. DOI:10.4103/jehp.jehp_508_21

[33] Liu Q, Qu X, Wang D, Abbas J, Mubeen R. Product market competition and firm performance: Business survival through innovation and entrepreneurial orientation amid COVID-19 financial crisis. Frontiers in Psychology [Internet]. 2022;12:790923. DOI:10.3389/fpsyg.2021.790923

[34] Crawford K. Halt the use of facial-recognition technology until it is regulated. Nature [Internet]. 2019;572(7771):565. DOI: 10.1038/d41586-019-02514-7

[35] Ringrose K. Law Enforcements Pairing of Facial Recognition Technology with Body-Worn Cameras Escalates Privacy Concerns. Va Law Rev. 2019;105:57-66.

[36] Stark L. Facial recognition is the plutonium of AI. Crossroads [Internet]. 2019;25(3):50-5. DOI: 10.1145/3313129

[37] Garvie C, Bedoya A, Frankle J. Washington: The perpetual line-up: unregulated police face recognition in America. Center on Privacy & Technology at Georgetown Law; 2018.

[38] Roussi A. Resisting the rise of facial recognition. Nature [Internet]. 2020;587(7834):350-3. DOI: 10.1038/d41586-020-03188-2

[39] Cavazos JG, Phillips PJ, Castillo CD, O'Toole AJ. Accuracy comparison across face recognition algorithms: Where are we on measuring race bias? IEEE Transactions on Biometrics, Behavior, and Identity Science. 2020;3(1):101-11. DOI: 10.1109/TBIOM.2020.3027269

[40] Buolamwini J, Gebru T. Gender shades: Intersectional accuracy disparities in commercial gender classification. In Conference on fairness, accountability and transparency. PMLR. 2018 Jan 21; 77-91.

[41] Algorithm Watch. AI ethics guidelines global inventory. Germany; 2020.

[42] Elo S, Kyngäs H. The qualitative content analysis process. J Adv Nurs. 2008;62(1):107-15. DOI: 10.1111/j.1365-2648.2007.04569.x

[43] Page MJ, McKenzie JE, Bossuyt PM, Boutron I, Hoffmann TC, Mulrow CD, et al. The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. BMJ [Internet]. 2021;372:n71. DOI: 10.1136/bmj.n71

[44] Farzadfar F, Naghavi M, Sepanlou SG, Saeedi Moghaddam S, Dangel WJ, Davis Weaver N,... Larijani B. Health system performance in Iran: A systematic analysis for the global burden of disease study 2019. The Lancet [Internet]. 2022. DOI:10.1016/s0140-6736(21)02751-3

[45] Neuendorf KA. The content analysis guidebook. Los Angeles (CA): Sage; 2016.

[46] Yao J, Ziapour A, Abbas J, Toraji R, NeJhaddadgar N. Assessing puberty-related health needs among 10-15-year-old boys: A cross-sectional study approach. Archives de Pédiatrie [Internet]. 2022;29(2). DOI:10.1016/j.arcped.2021.11.018

[47] United Nations. Universal declaration of human rights. New York (NY).

[48] Geraghty L. Facial recognition report [Internet]. National League of Cities. Available from: https://www.nlc.org/wp-content/uploads/2021/04/NLC-Facial-Recognition-Report.pdf. [Accessed 16 July 2021].

[49] SAFR. Privacy by design: best practices for using facial recognition to support safer K-12 campuses. Seattle (WA); 2018.

[50] United States Chamber of Commerce, Chamber Technology Engagement Center. Facial recognition policy principles. Washington (DC); 2019.

[51] Integrated Justice Information Systems Institute and the International Association of Chiefs of Police, Law Enforcement Imaging Technology Task Force. Guiding principles for law enforcement's use of facial recognition technology. Alexandria (VA); 2019.

[52] Federal Bureau of Investigation. Facial recognition technology: ensuring transparency in government use (testimony of Kimberly J. Del Greco). Washington (DC); 2019.

[53] Greene J. Can facial recognition technology be used ethically? [Internet]. Imageware Blog. 2020. Available from: https://blog.imageware.io/can-facial-recognition-technology-be-used-ethically. [Accessed 16 July 2021].

[54] World Economic Forum. A framework for responsible limits on facial recognition use case: flow management. Geneva; 2020.

[55] West DM. 10 actions that will protect people from facial recognition software [Internet]. Brookings. 2019. Available from: https://www.brookings.edu/research/10-actions-that-will-protect-people-from-facial-recognition-software/. [Accessed 16 July 2021].

[56] Future of Privacy Forum. Privacy principles for facial recognition technology in commercial applications. Washington (DC); 2018.

[57] United States Department of Justice, Bureau of Justice Assistance. Face recognition policy development template. Washington (DC): Bureau of Justice Assistance; 2017.

[58] Security Industry Association. SIA principles for the responsible and effective use of facial recognition technology. Silver Spring (MD); 2020.

[59] Facial Identification Scientific Working Group. Facial identification practitioner code of ethics (Version 2.0). Washington (DC); 2018.

[60] Association for Computing Machinery, U.S. Technology Policy Committee. Statement on principles and prerequisites for the development, evaluation, and use of unbiased facial recognition technologies. New York (NY); 2020.

[61] Algorithmic Justice League, Center on Technology and Privacy at Georgetown Law. Safe face pledge. Cambridge (MA); 2018.

[62] American Legislative Exchange Council. Statement of principles on facial recognition policy. Arlington (VA); 2021.

[63] United States Department of Commerce, National Telecommunications and Information Administration. Privacy best practice recommendations for commercial facial recognition use. Washington (DC); 2016.

[64] Montgomery C, Hagemann R. Precision regulation and facial recognition. Ibm.com. 2019. Available from: https://www.ibm.com/blogs/policy/facial-recognition/. [Accessed 16 July 2021].

[65] Google. Our approach to facial recognition [Internet]. Mountain View (CA). Available from: https://ai.google/responsibilities/facial-recognition/. [Accessed 16 July 2021].

[66] Microsoft Corporation. Six principles for developing and deploying facial recognition technology. Redmond (WA); 2018.

[67] Vilimek J. Key considerations for the ethical use of facial recognition technology [Internet]. Avanade.com. 2019. Available from: https://www.avanade.com/en/blogs/avanade-insights/artificial-intelligence/ethical-use-of-facial-recognition. [Accessed 16 July 2021].

[68] Axon AI Ethics Board, Policing Project at NYU School of Law. First report of the Axon AI ethics board: face recognition. New York (NY); 2019.

[69] Punke M. Some thoughts on facial recognition legislation [Internet]. Amazon Web Services. 2019. Available from: https://aws.amazon.com/blogs/machine-learning/some-thoughts-on-facial-recognition-legislation/. [Accessed 16 July 2021].

[70] Goldman P. Why we've never offered facial recognition [Internet]. Salesforce. 2020. Available from: https://www.salesforce.com/news/stories/why-weve-never-offered-facial-recognition/. [Accessed 16 July 2021].

[71] Sakpal M. How to use facial recognition technology responsibly and ethically [Internet]. Gartner.com. 2020. Available from: https://www.gartner.com/smarterwithgartner/how-to-use-facial-recognition-technology-responsibly-and-ethically/. [Accessed 16 July 2021].

[72] Wang C, Wang D, Abbas J, Duan K, Mubeen R. Global financial crisis, smart lockdown strategies, and the COVID-19 spillover impacts: A global perspective implications from southeast Asia. Frontiers in Psychiatry [Internet]. 2021;12(1099):643783. DOI: 10.3389/fpsyt.2021.643783

[73] Abbas J, Wang D, Su Z, Ziapour A. The role of social media in the advent of COVID-19 pandemic: Crisis management, mental health challenges and implications. Risk Management and Healthcare Policy [Internet]. 2021;14:1917-32. DOI: 10.2147/RMHP.S284313

[74] NeJhaddadgar N, Ziapour A, Zakkipour G, Abolfathi M, Shabani M. Effectiveness of telephone-based screening and triage during COVID-19 outbreak in the promoted primary healthcare system: A case study in Ardabil province, Iran. Z Gesundh Wiss [Internet]. 2020;29:1-6. DOI:10.1007/s10389-020-01407-8

[75] Creswell JW, Creswell JD. Research design: Qualitative, quantitative, and mixed methods approaches. Thousand Oaks, CA: SAGE Publications; 2018.

[76] Flick U. An introduction to qualitative research an introduction to qualitative research. 6th ed. London, England: SAGE Publications; 2019.

[77] Shkedi A. Data analysis in qualitative research: practical and theoretical methodologies with optional use of a software tool. Seattle (WA): Amazon; 2019.

[78] Korstjens I. Moser A. Series: Practical guidance to qualitative research. Part 4: Trustworthiness and publishing. Eur J Gen Pract [Internet]. 2018;24(1):120-4. DOI: 10.1080/13814788.2017.1375092

[79] Hsieh H-F, Shannon SE. Three approaches to qualitative content analysis. Qual Health Res [Internet]. 2005;15(9):1277-88. DOI: 10.1177/1049732305276687

[80] White MD, Marsh EE. Content Analysis: A Flexible Methodology. Libr Trends [Internet]. 2006;55(1):22-45. DOI: 10.1353/lib.2006.0053