Documenting the Undocumented: Privacy and Security Guidelines for Humanitarian Work with Irregular Migrants

Sara Vannini[1], Ricardo Gomez[2], and Bryce Clayton Newell[3]

[1] University of Washington, Dept. of Communication, vanninis@uw.edu
[2] University of Washington, Information School, rgomez@uw.edu
[3] University of Kentucky, School of Information Science, brycenewell@uky.edu

Abstract. Humanitarian organizations frequently do not fully address the implications of collecting, storing, and using data about vulnerable populations. We propose a conceptual framework for Humanitarian Information Activities (HIA), especially in the context of undocumented migration. We examine this framework in the light of both a survey of the literature and a pilot study that examines HIA activities in three distinct contexts: 1) higher education institutions that provide support to undocumented students, 2) non-profit organizations that provide legal support to undocumented immigrants, and 3) humanitarian organizations assisting undocumented migrants near the US-Mexico border. We discuss both technological and human risks in HIA, the limitations of privacy self-management, and the need for clear privacy-related guidelines for HIA. We conclude suggesting guidelines to strengthen the privacy protection offered to vulnerable populations by humanitarian organizations in the context of irregular migration.

Keywords: privacy, data justice, humanitarian information activities, migration.

1 Introduction

Migration and privacy crises are central topics of public discourse today, but they are only recently starting to be addressed together [1]. The growing and continuing displacement and transnational migration of millions of people around the world has been met with increased surveillance and "datafication of migration" by a variety of actors [2], [3]. Because migrants, humanitarian organizations, and governments are increasingly using digital technologies to facilitate, support, or regulate migration, migrants are increasingly leaving "digital traces of their migration" [3], [4]. Governmental institutions and humanitarian organizations are utilizing a variety of information and communication technologies (ICTs) as part of migration-related operations without any widely accepted approach for ensuring that human rights are respected throughout these information-rich activities [5].

In the context of humanitarian organizations, all "activities and programs which may include the collection, storage, processing, analysis, further use, transmission, and public release of data and other forms of information by humanitarian actors and/or affected communities" are defined by Greenwood et al. [5, p. 5] as Humanitarian Information Activities (HIA). Although humanitarian organizations often focus on helping migrants during times

of personal crisis, they frequently overlook the additional vulnerabilities and unintended risks that the careless collection, storage, and use of personal information about migrants can cause. This can happen at the macro level, due to the general datafication of migration, or at the micro level (for example, during intake interviews at migrant shelters or legal-aid centers). In the humanitarian sector, these HIA-related activities are often pursued as forms of surveillance as care [6, pp. 33–34], [7].

ICTs can help organizations make their work more efficient and effective, and they can help the populations they serve by providing them access to relevant information and services. However, the use of ICTs also involves data- and privacy-related risks, as electronic data can be subjected to security breakages, leaks, hacks, inadvertent disclosure, and disclosure through legal processes (e.g., subpoenas, court orders). In certain cases, the inadvertent or malicious exposure of personal data can significantly exacerbate the risks for particularly vulnerable populations. In the case of undocumented migrants, disclosure of sensitive information and documents may expose them to detention, deportation, and other forms of physical and psychological violence. Nevertheless, the efforts organizations are making to protect the personal information of the individuals they serve, and the remaining risks related to their HIA have not been widely investigated in academic research.

The recommendations we propose echo the approach of the European Union's General Data Protection Regulation (GDPR), which now imposes significant legal obligations on humanitarian organizations to comply with strict data protection rules [7], [8].

The remainder of the paper is organized as follows: first, we briefly review related work in scholarly literature on humanitarian action related to migration and HIA. Second, we present the methodology for our work. Third, we discuss the review of the literature in contrast to the interviews. Finally, we conclude with a proposed framework and recommendations to strengthen the privacy protections in HIA-related work by humanitarian organizations serving undocumented migrants and other vulnerable populations.

2 HIA-related risks and humanitarian intervention

Humanitarian organizations provide humanitarian assistance for populations that are particularly vulnerable and deprived of their human rights. This includes humanitarian organizations that work with undocumented migrants in the US. When migrants arrive in the US fleeing from violence, climate change-related disasters, or lack of opportunities in their home countries, they frequently cross the border without authorization. They are labeled as "illegal aliens" and, as undocumented people in the country, they have almost no legal path to legalize their situation: they have limited rights, limited possibilities to appeal when abused, and limited legal access to basic societal services, such as education, healthcare, and the formal job market [9]–[11]. They are mostly doomed to live abjected lives [9] and in a "state of exception" [12].

For humanitarian organizations working with undocumented immigrants, coordinating humanitarian relief presents many challenges, many of which are rooted in lack of funding,

conflicting organizational goals, professional and organizational status hierarchies, and the tendency of individual organizations to maximize their own autonomy [13]. They frequently do not prioritize the protection of information and privacy rights of the populations they serve. Greenwood et. al [5] point to a disconnect between theory and practice to effectively alleviate humanitarian organizations' HIA-related risks in an exhaustive and coordinated manner, showing how HIA conducted through the use of ICTs may cause harm and violate the basic human rights of the vulnerable populations the organizations are assisting. These issues tend to exacerbate the vulnerability of undocumented migrants, whose status already places them at risk.

There is a striking lack of generally accepted protocols and measures in place to ensure the privacy and protection of vulnerable people within the humanitarian space: for example, while the Signal Code promulgated by the Harvard Humanitarian Initiative offers "guidance on articulating the human rights relating to information and data" [5, p. 9], specifically addressing HIA, the commonly used Core Humanitarian Standard on Quality and Accountability [14] does not address privacy protections or on the implications of privacy disclosures as part of its standards. Furthermore, both frameworks are addressed to organizations working with populations affected by short-term crises but fail to include the specific challenges of dealing with people such as undocumented migrants or refugees, whose crises are usually more long-term.

3 Methodology

In the fall of 2017, we conducted a small set of interviews (n=9) with staff and volunteers of humanitarian organizations working with undocumented migrants in the US, in order to assess their awareness and practices regarding the protection of information and privacy of the people they serve. We interviewed five staff members in different roles from four different advocacy groups, and four from two higher education institutions on the US West Coast. Interviewees included executive directors, coordinators, legal advisors and Information Technology department directors. We identified three emerging themes in the literature review, and used these to code and analyze the interviews using a double content analysis process: a first bottom-up phase aimed to identify thematic areas and recurrent topics with the help of qualitative analysis software Dedoose; and a second phase including a top-down approach, moving from the first thematic areas identified to a structure reflecting the three themes emerging from the literature review. Finally, we collected admissions and enrollment forms, flyers, web sites, videos, and online forms, and observed social media pages with the aim to better understand the practices of the organizations involved.

This is an exploratory study of a novel topic. The sample size is small, so it is not necessarily representative of all HIA practices, but it offers valuable insight for future work in this area. We report the results of the interviews using aggregate organizational personas, to protect our interviewees' privacy and the organizations' operations. Thus, "University of Nepantla" will represent the persona for the for the two higher education institutions, and

"La Resaca" the aggregate organizational persona for the four interviewed advocacy groups.

4 HIA in theory: A review of the literature on HIA

Our review of the literature identified three key trends related to HIA-related risks and different levels of awareness and security practices connected to them. First, risks are related to both *technology* (inadequate or low-quality security systems, poor routine maintenance practices, loose internal controls, and an underutilization of necessary protection tools and services) and *human behavior* (improper training amongst organizations, poor onboarding and offboarding practices, limited knowledge resources available to the organization, and even poorly engaged staff). Second, there is a *lack of clear guidelines* (reflecting a corresponding need to implement them) on how to deal with data and information. Finally, organizations need to develop strategies that go *beyond the logic of privacy self-management*. The following sections discuss these three trends in relation to related work in the specialized literature.

4.1 HIA-related risks involve both technology and people

One of the primary issues that organizations engaging with technology must deal with is data security. The risk of data breakages, hacks, and leaks are a reality not only in the corporate and governmental worlds. In the wake of cybercrime attacks, cyber-warfare, and with more (and more sophisticated) interception and surveillance technology available to governments, the United Nations Office for the Coordination of Humanitarian Affairs (OCHA) has been vocal about concerns for humanitarian organizations' data systems and online activity [15]. Often, the inability of humanitarian organizations to introduce proper safeguards is tied to limited resources, and this is particularly true for smaller humanitarian organizations operating only at a local level. The costs of complex security technologies and properly trained personnel are often difficult for these organizations to afford or justify. Risks to the information privacy of vulnerable populations can also be increased by human factors (e.g., negligently handling information, whether willfully or not). Internal controls and plans to improve workers' knowledge and best practices are necessary but often missing [16].

4.2 Clear guidelines for HIA are needed, especially in the context of migration

Greenwood et. al [5, p. 61] state that there are "gaps in international humanitarian and human rights law and standards around humanitarian information activities." Based on the idea that information is a basic "humanitarian need," they advocate for the adoption of "minimum ethical and technical standards for HIA, grounded in an accepted foundation of human rights standards and international law" [5, p. 5]. They identify five rights of all people related to HIA based on three criteria: (i) they fit in with existing declarations, laws or

conventions relevant to human rights; (ii) they apply to all people independently of technology, and (iii) they reinforce and translate existing rights into the specific context of HIA. These five rights are: *Right to Information*, *Right to Protection* from threats and harms, *Right to Privacy and Security*, *Right to Data Agency*, and *Right to Redress and Rectification* [5, p. 13]. Each one of these rights also applies to the protection of migrants, and especially the most vulnerable (asylum seekers, refugees, or irregular and undocumented migrants).

Current approaches to data protection within HIA are insufficient, as no comprehensive doctrine guiding the execution of HIA in accordance with ethical codes of conduct, rules, laws, or policies exists [17], [18], nor are accountability measures and auditing entities in place—even the European Union's pioneering protection of "data subjects" under the General Data Protection Regulation (GDPR) [19, Para. 4] suffers from limitations in this regard (e.g., its jurisdiction is limited to EU member states).

4.3 Privacy self-management is not enough

Privacy self-management rests on the idea that individuals need to control access to, as well as the use and retention of, their personal data through choosing to consent or not to privacy-related terms, conditions, and agreements. Privacy self-management promotes a notion of an informed user being able to make decisions about giving or withholding consent to the collection, use, and disclosure of personal data, including short and long-term consequences of such consent, in their best self-interest [20].

Although privacy self-management might resonate with the idea of empowering people to make their own choices, scholars recognize that its use is problematic and has been pushed "beyond its limits" [20, p. 1903]. Solove [20] identifies a number of cognitive and structural problems that fault privacy self-management, which prevent people's ability to truly weigh the costs and benefits of consenting.

5 HIA in practice: Interviews with staff and volunteers

In this section, we present the results of interviews in the form of narratives of organizational personas, which aggregate the findings and protect the identity of the informants.

5.1 HIA-related risks involve both technology and people

University of Nepantla: The "University of Nepantla" prohibits ICE from entering campus to conduct immigration raids or locate undocumented students. Sensitive personal information at the university is stored on a secure multi-authentication system server which gives many students peace of mind. A closer audit of the security and authentication of the information systems in use, and of the staff training for awareness and compliance with privacy and security protocols, though, could help strengthen the HIA-related practices of the university. The institution leverages technology to safeguard undocumented students who attend widely photographed events (where the risk that photos might be published and tagged

on social media is heightened). They have a low-tech method of helping students to avoid cameras if they want, consisting of providing large wearable stickers as a signal that they wish to not be photographed. This system is not infallible, and a coordinator makes sure to check photos that are posted online.

La Resaca: Organizers at the non-profit organization "La Resaca" regret that they don't have enough funding to implement highly secure information systems. "La Resaca" is a small organization and cannot afford to have as much internal staffing dedicated exclusively to creating, securing, and maintaining their servers as some larger organizations. Thus, they rely primarily on volunteer labor, free online services and document management systems, and basic (if any) encryption protections. Third-party services often manage and store their databases to guarantee the data is secured. Third-party organizations are also responsible for addressing any security problems that arise. However, the privacy policies of these organizations are mostly not questioned by "La Resaca." "La Resaca" has considered moving their sensitive data to overseas servers, where information would be stored beyond the jurisdiction of the US government, and to formulate other strategies for improving data security.

"La Resaca" generally uses both paper and electronic methods to collect and store data. This is usually determined by client preferences, the affordability of technologies available to them, and staff expertise. Information that requires high levels of accuracy, such as anything related to people's legal status, is usually duplicated in both electronic and paper files. The organization normally decides to convert the paper documents into electronic form only when they are sure that they will continue working with a person. Otherwise, the initial information is collected only on paper and then shredded. The organization is reluctant to choose one way of storing data over the other.

5.2 Clear guidelines for HIA are needed, especially in the context of migration

Protections at University of Nepantla: At the "University of Nepantla," staff members are aware of the possibility of unwilling disclosure of sensitive information, either because of failure of technologies used within the organization or because of human errors and obliviousness in evaluating information disclosure. Obliviousness, in some cases, includes misunderstanding the privacy laws (e.g., FERPA) to which institutions are required to adhere. Only higher-ranking staff members, in fact, do receive training on FERPA and in privacy and security. According to our data, staff members who did not receive any training usually err on the side of caution and mention letting the students themselves be the ones who actively protect their own security. Also, members of the staff usually rely on previous personal knowledge and self-training to compensate for the lack of formal on-the-job data protection training. Similarly, no structured training is set up when dealing with student volunteers that help manage services.

Protections at La Resaca: Legal standards affect the work of non-profits like "La Resaca." However, non-profits normally do not have concrete sets of privacy standards or

provide privacy-related training to their employees and volunteers. Staff members usually provide answers to questions that arise organically in their work, based on the unique needs of their clients. Occasionally, they might invite speakers to present about specific privacy issues that arise in their work.

5.3 Privacy self-management is not enough

Most of the organizations in our study discussed giving the undocumented individuals the agency to decide regarding their own privacy. Supporting entities and departments at the "**University of Nepantla**" mostly leave it up to the students themselves to disclose their undocumented status, except when it comes to matters of tuition and financial aid. In very few cases, Facebook groups hosted by the institution are closed to outsiders, and access is restricted to verified students that participate in in-person activities; the group moderator emphasizes the importance of privacy settings and behaviors, but ultimately, each student manages their own online presence, privacy settings and self-disclosure.

However, staff at all the organizations we spoke with declared that it is a priority for them to respond to any privacy concerns their clients had by explaining the way they do address privacy issues. For example, at the "University of Nepantla," staff explain the security protocols that are in place and the institutional obligations to each student individually. "**La Resaca**" works in a similar fashion. Lawyers and staff members dedicate time to their clients to make sure they understand what they are agreeing to, as well as the measures they can take if their confidentiality is not respected.

6 Discussion and recommendations

Humanitarian organizations may not be doing enough to protect the information privacy of vulnerable populations in the context of irregular migration, and they may lack solid, agreed-upon best practices to draw from. Humanitarian organizations frequently fail to address both the technical and human-factor risks presented by even the most basic information systems they use to collect, process, and store information about vulnerable populations. They employ no clear and commonly accepted guidelines for protection of information of vulnerable populations. This might have several possible different consequences for how data will be handled in the case of requests from external entities, which include the disclosure of sensitive information inadvertently by untrained staff members and volunteers. Furthermore, there are no entities in charge of promoting and holding organizations accountable for their information practices, especially in the context of irregular transnational migration. Well-known guidelines for HIA-related accountability [5][14] were not widely known within or adopted by the organizations we studied. Even though these guidelines fail to explicitly address information privacy and data security, they do provide standards for HIA which organizations did not, however, adopt.

Based on this analysis, we suggest the **HIA Privacy Guidelines** (summarized in Table 1, below) to strengthen the privacy protection by humanitarian organizations working in the

context of irregular migration. These guidelines invite humanitarian organizations to collect as little personal information as possible to conduct their work, to better protect such information from technical and human risks of disclosure, to train their staff and volunteers in secure data collection and management, to work with other organizations that share in these basic privacy principles for HIA, and to make sure they provide their services even to those individuals that might decide to opt-out from complying and sharing information about themselves, either digitally or at all. These recommendations also clearly outline possible areas for future collaboration between humanitarian organizations, academic researchers, and technologists. Future work needs to test and refine these proposed guidelines.

Table 1. Privacy Guidelines for Humanitarian Information Activities (HIA)

HIA Privacy Guidelines Guidelines to strengthen privacy protections in the context of irregular migration.
PRUDENCE: Collect as little information as possible
PROTECTION: Secure the information you do need to collect and store
TRAINING: Make sure volunteers and staff are aware and trained on privacy protection; help your users be more privacy aware
SHARE ALIKE: Work with collaborators and partners who share your concern
NON-DISCRIMINATION: Offer services to all, including those who do not want to share their personal information

The mass forced migration of people around the world has become a particularly difficult challenge of our time. Due to the significant risks potentially imposed on these vulnerable populations through the collection, analysis, and dissemination of personal (or personally-identifiable) information, humanitarian organizations must take responsibility for the implications of the data they collect about their intended beneficiaries. Otherwise, the best intentions of humanitarian organizations may well exacerbate the vulnerability of the very populations they intend to serve. Information is like toothpaste: once it is out of the tube, it is almost impossible to get it back in.

References

[1] C. Maitland, S. Braman, and P. T. Jaeger, *Digital Lifeline?: ICTs for Refugees and Displaced Persons*. MIT Press, 2018.

[2] D. Broeders and H. Dijstelbloem, "The Datafication of Mobility and Migration Management: the Mediating State and its Consequences.," in *Digitizing Identities: Doing Identity in a Networked World*, I. van der Ploeg and J. Pridmore, Eds. Routledge, 2016, pp. 242–260.

[3] G. Garelli and M. Tazzioli, "Migrant Digitalities and the Politics of Dispersal: An Introduction," *Border Criminologies Blog, Oxford Law Faculty*, 22-May-2018. .

[4] D. Broeders, *Breaking Down Anonymity: Digital Surveillance of Irregular Migrants in Germany and the Netherlands*. Amsterdam: Amsterdam University Press, 2009.

[5] F. Greenwood, C. Howarth, D. Escudero Pool, N. A. Raymond, and D. P. Scarnecchia, "The Signal Code: A Human Rights Approach to Information During Crisis," Harvard, MA, 2017.

[6] B. C. Newell, R. Gomez, and V. E. Guajardo, "Information seeking, technology use, and vulnerability among migrants at the United States–Mexico border," *The Information Society*, vol. 32, no. 3, pp. 176–191, May 2016.

[7] rbharani, "The GDPR is a unique opportunity to get humanitarian data protection right.," *The Digital Responder*, 30-Dec-2017. .

[8] S. Pfeifle, "Doing data protection well in humanitarian efforts," *The International Association of Privacy Professionals: the privacy advisor.*, 25-Oct-2017. .

[9] R. G. Gonzales and L. R. Chavez, "'Awakening to a Nightmare': Abjectivity and Illegality in the Lives of Undocumented 1.5-Generation Latino Immigrants in the United States," *Current Anthropology*, vol. 53, no. 3, pp. 255–281, 2012.

[10] S. A. D. Miller, "Faith Based Organizations and International Responses to Forced Migration," in *The Changing World Religion Map*, Springer, Dordrecht, 2015, pp. 3115–3133.

[11] G. Noll, "Why Human Rights Fail to Protect Undocumented Migrants," *European Journal of Migration and Law*, vol. 12, 2010.

[12] G. Agamben, *Homo Sacer: Sovereign Power and Bare Life*, 1st ed. Standford, CA: Stanford University Press, 1998.

[13] D. J. Saab *et al.*, "Building global bridges: Coordination bodies for improved information sharing among humanitarian relief agencies.," in *Proceedings of the 5th International ISCRAM Conference*, Washington, DC, USA, 2008.

[14] CHS Alliance, Groupe URD, and The Sphere Project, "Core Humanitarian Standard: Core Humanitarian Standard on Quality and Accountability," 2014.

[15] D. Gilman and L. Baker, "Humanitarianism in the Age of Cyber-warfare: Towards the Principled and Secure Use of Information in Humanitarian Emergencies," United Nations Office for the Coordination of Humanitarian Affairs, OCHA Policy Development and Studies Branch, 011, 2014.

[16] A. Kohnke, D. Shoemaker, and K. E. Sigler, *The Complete Guide to Cybersecurity Risks and Controls*. CRC Press, 2016.

[17] N. Raymond, Z. Al Achkar, S. Verhulst, J. Berens, and L. Barajas, "Building data responsibility into humanitarian action," OCHA - United Nations Office for the Coordination of Humanitarian Affairs, 18, 2016.

[18] N. A. Raymond, B. Card, and Z. al Achkar, "What is 'Humanitarian Communication'? Towards Standard Definitions and Protections for the Humanitarian Use of ICTs," European Interagency Security Forum (EISF), 2015.

[19] GDPR, *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, vol. L119. 2016.

[20] D. J. Solove, "Introduction: Privacy Self-Management and the Consent Dilemma," *Harvard Law Review*, vol. 126, no. 7, pp. 1880–1903, 2013.