Privacy and Security Guidelines for Humanitarian Work with Undocumented Migrants

Sara Vannini
Department of Communication
University of Washington
Seattle, WA, USA
vanninis@uw.edu

Ricardo Gomez
Information School
University of Washington
Seattle, WA USA
rgomez@uw.edu

Bryce Clayton Newell
School of Information Science
University of Kentucky
Lexington, KY, USA
brycenewell@uky.edu

ABSTRACT

Based on preliminary work with humanitarian organizations working with migrants in the US, we propose a set of Privacy Guidelines for Humanitarian Information Activities (HIA), in the context of undocumented migration. We discuss both technology and human risks in HIA, the limitations of privacy self-management, and the need for clear guidelines for HIA, such as the ones we tentatively suggest here.

CCS CONCEPTS

• H.0 General • J.4 SOCIAL AND BEHAVIORAL SCIENCES

KEYWORDS

Data privacy, data justice, humanitarian information activities, migration.

ACM Reference format:
Sara Vannini, Ricardo Gomez, Bryce Clayton Newell. 2019. Privacy and Security Guidelines for Humanitarian Work with Undocumented Migrants. In *Tenth International Conference on Information and Communication Technologies and Development (ICTD '19), January 4–7, 2019, Ahmedabad, India. ACM, New York, NY, USA, 2 pages.* https://doi.org/10.1145/3287098.3287120

1 Introduction

Humanitarian Information Activities are 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" [1]. 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. 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" [2], [3].

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. In this poster we discuss some of the themes identified in the literature, and the practices that emerge in a preliminary study of humanitarian organizations working with undocumented migrants in the US. We present a set of practical, normative recommendations that humanitarian organizations can adopt to better protect the privacy and security of the vulnerable populations they serve while still allowing them to do their important humanitarian work.

2 Related work

According to the United Nations High Commissioner for Refugees (UNHCR), we are now witnessing the highest numbers of human displacement ever recorded. In 2016 alone, an unpreceded 65.6 million people were forced to migrate worldwide. In Central America, the number of people

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

ICTD '19, January 4–7, 2019, Ahmedabad, India. 2019 Copyright held by the owner/author(s). Publication rights licensed to ACM.
ACM ISBN 978-1-4503-6122-4/19/01. . . $15.00

fleeing from gang violence and organized criminality has grown by ten times in just the past 5 years. Projections expect these numbers to increase [4].

For humanitarian organizations working with undocumented immigrants, coordinating humanitarian relief and action presents many challenges, many of which are rooted in lack of funding, conflicting organizational goals and missions, professional and organizational status hierarchies, and the tendency of individual organizations to maximize their own autonomy [5].

Greenwood et. al [1] point to a disconnect between theory and practice to effectively alleviate humanitarian organizations' HIA-related risks in an exhaustive and coordinated manner, pointing out how HIA conducted through the use of ICTs may cause harm and violate the basic human rights of the vulnerable populations humanitarian organizations are assisting. Furthermore, 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 offers "guidance on articulating the human rights relating to information and data" [1, p. 9], specifically addressing HIA, the commonly used Core Humanitarian Standard on Quality and Accountability [6] does not include any information on privacy protections or on the implications of privacy disclosures as part of its standards.

Our review of related work identified three trends:

(1) HIA-related risks involve both technology and people: Data security involves technical risks of leaks, hacks and other attacks that humanitarian organizations frequently don't have the technical know-how or resources to prevent [7]. But risks to the information privacy of vulnerable populations can also be increased by the human factor, as a result of negligently handling information, whether willfully or not. Internal controls and plans to improve organizational workers' knowledge and best practices are necessary but often missing [8][9], [10].

(2) Need for clear guidelines for HIA: Greenwood et. al [1] state that there are "gaps in international humanitarian and human rights law and standards around humanitarian information activities." The issue of informed consent to allow collection and storage of personal data of vulnerable populations is of particular concern [11]. Current approaches to (especially digital) data protection rights within HIA are insufficient [12], [13].The European Union (EU) pioneered the protection of "data subjects," defined within the General Data Protection Regulation (GDPR) [14]. Nonetheless, there is a lack of a single accepted definition of accountability in the humanitarian context, and the absence of generally accepted HIA practices (particularly when applied to transnational or irregular migration).

(3) Privacy self-management is not enough: 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 [15]. 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" [15]. For undocumented migrants trying not to disclose their status, privacy is particularly critical in an adverse social, economic, and legal environment. Not only are the risks of ill-informed or non-careful decisions higher, but the chances that populations that are already vulnerable will indeed make ill-informed or non-careful decisions are also higher. In particularly vulnerable situations, people might not have the ability to opt-out, as their data is required in return for basic services that they need more urgently and in the short term [16], [17].

3 Methodology

In the fall of 2017, we conducted a pilot study to investigate HIA among organizations working with undocumented migrants in the US, and to assess their awareness and practices regarding the protection of information and privacy of the people they serve. We interviewed five staff members from four different advocacy groups,[1] and four staff members from two higher education institutions[2] on the US West Coast, for a total of nine interviews. The interviewees had different roles in the organizations involved, so our outcomes express the opinions of executive directors, coordinators, legal advisors and Information Technology department directors.

[1] Organizations included in our study, represented by the organizational persona "La Resaca:" Northwest Immigrant Rights Project (NWIRP) (the largest non-profit immigrant rights organization focusing on low-income clients in the US, the Immigration Counseling Service (ICS)), a non-profit organization that provides legal services to immigrant communities, El Rescate (a small non-profit organization specialized in legal and financial services for immigrants), and the Washington Immigrants Solidarity Network (WAISN) (an all-volunteer coalition of groups specializing in assistance to immigrants and providing tools for immediate reporting of and response to Immigration and Custom Enforcement (ICE) activity).

[2] University of Washington and at Seattle Central College, including the Samuel E. Kelly Ethnic Cultural Center (ECC) within the Office of Minority Affairs and Diversity, Leadership Without Borders (LWB), a peer support group limited to undocumented students, and the DREAMERS Support Navigator that serves undocumented students at Seattle Central College.

4. Preliminary Findings

We present our findings as aggregate organizational personas, to protect our interviewees privacy and the organizations' operations. Thus, "La Resaca" will represent the aggregate organizational persona for the four interviewed advocacy groups, and "University of Nepantla" the one for the higher education institutions.

4.1 HIA-related risks involve both technology and people

The "University of Nepantla" operates as a public institution of higher education that commits itself to being a "sanctuary college" in the US. 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.

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."

4.2 There is a need for clear guidelines for HIA, especially in the context of migration

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. This has potentially a number of 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. 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.

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. In some cases, and especially in organizations slightly larger than "La Resaca," privacy training is done because it is required by funders. At times, staff members also receive training through other sources.

4.3 Privacy self-management is not enough

Most of the organizations in our study discussed giving the undocumented individuals the agency to make a decision 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. In other cases, though, even public social media spaces are considered places for students to be able to "come out" and be open about their stories as undocumented individuals if they wish to do so. Furthermore, staff members do not feel they have the right to tell them what they should and should not do. Social media are seen as platforms for activism and peer-support, as was evidenced in the national outrage against the termination of DACA protections and the protests surrounding the separation of minors from their parents, among other recent migration issues [18], [19].

However, staff at all of 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. They also provide handouts to their clients that outline the relevant

laws and regulatory policies they are adhering to, including the principle of attorney-client privilege. However, some staff described concerns about the low literacy rates of their clients, and that their clients may not have access to the tools, knowledge, and resources needed to make appropriate decisions regarding their own interests.

5. 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.

Based on this analysis, we argue that humanitarian organizations serving migrant populations should explicitly consider and develop internal **privacy and security-related protocols** (encompassing general information practices and the use of technology) to guide the work of their employees and volunteers. More specifically, these protocols should adhere to the following five guidelines:

1. Exercise prudence (limit the collection of personal information to include only information that is necessary);

2. Protect and secure information collected from and about migrants (paying attention to mitigating risks from both technological and human factors);

3. Provide training to ensure that volunteers and staff are aware and trained regarding the organization's privacy- and security-related protocols, and to empower users/clients to be more privacy aware);

4. Share-alike (work with collaborators and partners to improve privacy and security practices, based on on-going evaluation and refinement), and,

5. Non-discrimination. Organizations need to provide humanitarian services to everybody, including those who prefer not to share their personal information.

Future work needs to test and refine these proposed principles. Additionally, there is room to push beyond these basic principles on at least two fronts: 1) accountability (creating and institutionalizing methods to hold humanitarian organizations more accountable for protecting personal information and sensitive data about the vulnerable populations they intend to serve), and 2) embedding data subjects' rights into humanitarian practices, including effective mechanisms informing and empowering migrants about their rights to know, correct, or withdraw information held about them by humanitarian organizations (in line with the data protection obligations of the GDPR).

REFERENCES

[1] 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.

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

[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] UNHCR, "Global Trends. Forced Displacement in 2016," UNHCR - United Nations High Commissioner for Refugees, 2017.

[5] 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.

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

[7] 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.

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

[9] J. Camfield, "Meet SAFETAG: Helping Non-Profits Focus on Digital Security," *Internews*, 2015. .

[10] R. Dette, "Do No Digital Harm: Mitigating Technology Risks in Humanitarian Contexts," 2017.

[11] P. Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization," Vol. 57, 2009.

[12] 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.

[13] 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.

[14] 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.

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

[16] V. Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. New York, NY: St. Martin's Press, 2018.

[17] A. E. Marwick and D. Boyd, "Privacy at the Margins| Understanding Privacy at the Margins—Introduction," *Int. J. Commun.*, vol. 12, no. 0, p. 9, 2018.

[18] A. Chomsky, "Immigrants' Rights Are Workers' Rights," *NACLA Rep. Am.*, vol. 49, no. 2, pp. 206–211, Apr. 2017.

[19] S. Gleeson and P. Sampat, "Immigrant Resistance in the Age of Trump.," *New Labor Forum*, vol. 27, no. 1, pp. 86–95, Jan. 2018.