
Article:
Vannini, S. orcid.org/0000-0003-1527-7494, Gomez, R., Lopez, D. et al. (6 more authors) (2020) Humanitarian organizations' information practices : procedures and privacy concerns for serving the undocumented. The Electronic Journal of Information Systems in Developing Countries, 86 (1). e12109. ISSN 1681-4835

https://doi.org/10.1002/isd2.12109

Humanitarian Organizations Information Practices: procedures and privacy concerns for serving the Undocumented

1. Introduction

Many organizations in the United States engage with undocumented individuals to help them secure the legal counseling, social services, and educational assistance that might otherwise be unattainable (Immigration Advocates Network & Idealware, 2016). Undocumented migrants in the country face a constant fear of detention and deportation, which causes them to feel insecure, transient and impermanent in the daily lives (Gomez & Vannini, 2017; Gómez & Vannini, 2015; Vannini, Gomez, & Guajardo, 2016). What efforts humanitarian organizations are making to protect the personal information of the individuals they serve have, however, been little investigated (see: Vannini, Gomez, & Newell, 2019). While recent developments in information technology alone would call for an evaluation of current information systems and practices, the need for such an evaluation is made more urgent by the current political climate in the United States. Undocumented youth who had previously seen a path to citizenship through the DACA (Deferred Action for Childhood Arrivals) program created by executive order under Obama now fear that they may be targets for deportation under Trump, who ended the program in September of 2017 and has called on Congress to draft new immigration legislation (National Immigration Law Center, 2017a). Under the current presidency, the number of ICE (Immigration and Customs Enforcement) officers has also tripled, the targets for deportation have expanded, and an end to federal funding for sanctuary cities (local administrations that do not collaborate with the federal administration to denounce and deport undocumented individuals) has been called for (National Immigration Law Center, 2017b). Because of these changes, the legal and social services offered by humanitarian information organizations have taken on greater importance in the lives of the undocumented, as has the obligation of these organizations to protect the privacy of the vulnerable populations they serve.

2. Literature review

Undocumented migrants in the United States experience complex relations with privacy, security and social activism, as their Information behaviors are mediated by the constant fear of detention and deportation in their daily lives (Vannini et al., 2016). In this study, we focus on humanitarian organizations that work with the undocumented in the country, and we aim to identify the information systems and practices currently used by these organizations to assess how they protect the privacy of the people they aim to serve.

Our interviews and document analyses were informed by several studies that are more technical or prescriptive in nature. First are two sets of guidelines, one by Colli-

er (Collier, 2017) and a second by Raymond (Raymond, Al Achkar, Verhulst, Berens, & Barajas, 2016), that suggest specific approaches to institutional audits of information systems and practices. In response to the crisis faced by "many of our students [who] are at risk of deportation, of brutality, of harassment," Collier urges academic institutions to restyle themselves as "digital sanctuaries" for student data, retaining as little information as possible on students, having clear protocols and training for the storage and sharing of data, and reconsidering the necessity of using third-party vendors such as providers of online course interfaces and the plagiarism detection service Turnitin (Collier, 2017). Raymond (Raymond et al., 2016) proposes a four-step process for information security audits by humanitarian organizations, briefly, evaluating the purpose for which data is generated and shared, taking inventory of the data, identifying risks, and developing strategies to minimize those risks. A wide-ranging study of technical developments in information security by Olijnyk (Olijnyk, 2015) identifies multiple sub-disciplines of the field, such as communication security, data security, and network security, and provides a bibliography for further research on each. Next are two articles that stress the continued importance of human interactions, real or virtual, in protecting the undocumented, and situations where low-tech methods of information management might actually be more secure. Both of these articles also stress the importance of training volunteers on the necessity of maintaining the privacy of the vulnerable populations they are trying to help (Cardia, Holzer, Xu, Maitland, & Gillet, 2017; Newell, Gomez, & Guajardo, 2016). Finally, a 2016 survey of immigrant rights organizations' information technology practices reveals several common weaknesses, particularly in the areas of data backup and password protocols (Immigration Advocates Network & Idealware, 2016).

Some undocumented individuals first experience the limits of their status as they enter higher education, an encounter made particularly challenging by the patchwork of federal and state regulations and institutional policies on admissions and financial aid for the undocumented (Gildersleeve, Rumann, & Mondragón, 2010). Since they are likely to be low-income, the first in their families to attend college, and at a higher risk for health and anxiety issues, these students typically require specialized assistance from multiple university departments, and will have to weigh the risks of revealing their status at each point of contact (Gildersleeve et al., 2010; Mendoza, 2016). If, through ignorance, indifference, or personal bias, administrators provide false or conflicting information or pass difficult questions off to other departments, the undocumented students' trust in the institution will be compromised, and his or her chances of academic success will be greatly reduced (Mangan, 2017; Mendoza, 2016). University staff who instead are trained to provide consistent and accurate information to the undocumented while maintaining their confidentiality can transform each disclosure of status into an empowering experience, a way for the undocumented to gain confidence and hope for the future after years of secrecy and mistrust (Muñoz, 2016).

The range of outcomes experienced by undocumented students in higher education is just one demonstration of the importance of uniform training of staff at all organizations that work with the undocumented, an idea that is born out in the literature. Researchers have shown the improved client outcomes provided by consistent training in social sensitivity (Ferguson, 2006; Mendoza, 2016), academic and legal advising (Gildersleeve et al., 2010; Mangan, 2017; Muñoz, 2016; Olivas, 2010), and

access to social services (Muhren, Eede, & Walle, 2009; Norris-Tirrell, 2014). In recent years, the particular importance training staff on the safe handling of sensitive client data has become a theme among researchers (Collier, 2017; Ferguson, 2006; Hollenhorst, 2017; Ritvo, 2016); it is possible that this trend has been brought about by the rapid development of new data management and communication technologies and the changing political climate.

An alternate response to the complications introduced by changing technologies and the new political climate is the idea of privacy self-management, allowing the undocumented to manage their own data and disclosure of immigration status (Solove, 2013). Out of confusion, overwork, or respect for client autonomy, staff at humanitarian organizations might leave privacy decisions to the undocumented. However, as Solove claims, the consent of the individual is insufficient in the age of big data, as it is not really possible for one's consent to truly be informed when the individual can no longer recognize and anticipate all the ways one's data might be shared and used by others (Solove, 2013). Even more when they are a particularly vulnerable population (Eubanks, 2018; Marwick & Boyd, 2018). It is therefore the responsibility of humanitarian organizations to advise the undocumented on the most cautious approach to personal information management.

3. Methodology

In this study, we were guided by two main research questions:

1. What are the information practices and systems employed by humanitarian organizations to protect the privacy of the undocumented individuals they serve?
2. How are they following legal standards and best technological practices regarding migrants' data privacy and security?

From the outset we sought to include a variety of organizations in our study from the US West Coast (States of California, Oregon and Washington), where the authors have established ties. We recognized that the needs of the undocumented change as they navigate the different legal, social service, and academic systems in the American society. Thus, we chose to focus on organizations that provide legal and academic services to migrants in the area with whom two of the authors had already established trust relationships in the previous years. We chose to work with four advocacy groups, the Northwest Immigrant Rights Project (NWIRP), the largest nonprofit immigrant rights organization focusing on low-income clients in the United States; Immigration Counseling Service (ICS), a nonprofit organization that provides easy access and affordable immigration legal services for immigrant communities in Oregon and Southwest Washington; the Washington Immigrants Solidarity Network (WAISN), an all-volunteer coalition of groups specializing in assistance to immigrants in the areas of education, labor, and social services, and providing tools for immediate reporting of and response to ICE activity in Washington; and El Rescate, a Los Angeles, California, based nonprofit organization that serves immigrants, in particular Latinos, in an effort to improve their political and economic status by providing legal and financial services and through community outreach. We also focused on

three organizations with ties to higher education, the admissions department at Seattle Central College and two groups at the University of Washington: the Samuel E. Kelly Ethnic Cultural Center (ECC) within the Office of Minority Affairs and Diversity; and Leadership Without Borders (LWB), a peer support group moderated by a university employee whose membership is limited to undocumented students.

Since our organizations were different in the work they are performing with undocumented migrants, two interview guides were written. For the five organizations that require some amount of personal information from the undocumented in order to provide assistance (NWIRP, ICS, WAISN, El Rescate, and Seattle Central College admissions), our questions focused on the systems and practices used to gather, store, and share that sensitive data. The two university support groups (ECC and LWB), instead, are outreach organizations that share information with their members and provide them with real and virtual social spaces; our interview questions for these two groups focused instead on the systems and practices (primarily Facebook) used to facilitate communication with and among the undocumented. We interviewed five staff members from the four advocacy groups, and four staff members from the two higher education institutions, for a total of nine interviews. The position of each interviewee was different in each organization, including executive directors, lawyers, technology directors, advocates and coordinators. Furthermore, a documents analysis was performed on admissions and enrollment forms, flyers, web sites, videos, online forms, and organizations' social media pages, with the aim to complement the data collected via the interviews.

4. Findings

4.1. Information systems and methods

In order to carry out their work, the nonprofit service organizations and the community college admissions department we investigated need to collect, filter, process, and share the personal information of their undocumented clients. We discovered that both paper and electronic forms and data storage methods were used by these organizations, as determined by client preferences, available technologies, and staff expertise. The peer support organizations at the University of Washington also use both paper and electronic systems to inform undocumented students of educational and social events. Usually general announcements appear on the public Facebook pages, while more specific event information, including the time and place of events, is conveyed through physical flyers posted in the more protected environment of the ECC.

The all-volunteer coalition WAISN exists primarily to facilitate monitoring and quick responses to ICE activity. The only client information the organization requires to carry out this service is phone numbers, which are stored on a listserv. Anytime ICE activity is reported and confirmed on the WAISN hotline, the location of the activity is announced to every number on the listserv. Organizations such as NWIRP, ICS, and El Rescate, however, need to maintain detailed files on their undocumented clients in order to help them manage their immigration cases. Collecting and storing personal information including employment and birth records on undocumented individuals applying for legal status or fighting deportation requires a high standard accu-

racy, completeness, and protection, usually achieved using both paper and electronic files. At ICS, potential clients fill out a paper intake form to determine if they might be eligible for services. If an individual's case is accepted, the information is then entered into a database. If a case is not accepted, the intake form is shredded.

Many non-profit humanitarian organizations rely on databases run by groups outside of their organization to store client data securely. ICS uses a database called Innovation Law Lab, which is provided to them for free due to their nonprofit status by the Immigrant Law Group. Law Lab is a cloud-based case management software that was designed by immigration lawyers for immigration lawyers, and therefore it is a client-focused, data-driven case management software. This database stores encrypted data in servers and allows for its secure transmission. Documents are made accessible anywhere there is an internet connection, eliminating the need for retaining duplicate paper records (https://innovationlawlab.org/blog/2017/07/05/why-innovation-law-lab-software-is-a-necessity-for-your-firm).

NWIRP uses a database called LegalServer. LegalServer is a web-based content management system that does not require any software installation. It provides secure remote access via the Internet and is accessible through standard internet browsers. LegalServer has its own team of database engineers, support staff and IT managers to assist the agencies it serves. Its users from within the legal system vary and include legal aid agencies, pro bono agencies, law schools, and immigration clinics, funding agencies, and public defenders (https://www.legalserver.org/features).

In both these cases, the outside group is responsible for updating the system and addressing any security problems that may arise. Other organizations, like El Rescate, use internally managed databases to store client information.

In addition to electronic files, the organizations maintain physical files for each client where they collect documents relevant to the client's immigration case, such as birth certificates, passports, court records, and medical records. At NWIRP, these documents are scanned into the electronic database when an application is sent to immigration.

The legal professional we interviewed expressed the importance of having case information both electronically and physically. According to one of the legal advocate interviewed, "it's good to have information both electronically and in a file... if the server's down, we have a copy available... or if we have the actual electronic copy and we can't find the paper copy, then it's very useful to have it in both places." One of the lawyers also stated that though it would be helpful for her work to move to an all-electronic system, there are certain advantages to the paper file that would make this change difficult:

> "I would like to go to all to like electronic [system] where we scan things in, then everything's in one place, but . . . I think that there's some kind of reluctance to do that because it's so hard to be sure [that the system hasn't been breached] with the electronic . . . I think for clients, most of [them] aren't computer literate or comfortable with computers at all, so I think they like to see… the physical paperwork."

Though an electronic system of data management might be more efficient for legal professionals, it is important to consider the ways in which clients perceive paper versus electronic methods. Undocumented individuals approaching humanitarian

organizations for assistance already sense themselves to be at risk. If their mistrust of technology makes them less willing to be forthcoming with personal information, the legal aid worker might not be able to obtain all the information needed to help the client.

4.2. Application of legal standards for privacy and protection

Legal standards play a key role in protecting the information of undocumented individuals within organizations and institutions. In legal organizations, these standards include the principle of attorney-client privilege, or the protection for lawyers from sharing sensitive information given to them by a client. The executive director of one of the organizations interviewed, shared:

> "Even if the government tried to subpoena information from us, because of the strength of the attorney-client privilege we've been generally able to fight off any attempts or threats of obtaining information about our clients. So we are able to reassure people about that and that obviously helps to . . . make sure people will share information with us."

This principle plays a key part in both keeping client information secure and ensuring that clients feel safe sharing with the organizations. Additionally, legal organizations must receive the consent of the client before sharing their information with a third party, and might be sanctioned if they violate these standards. One of the lawyers shared they often reassure clients by informing them of measures they can take if their confidentiality is not respected:

> "I explain to them that if they ever find out that I gave their information to somebody without their permission, that they can call this number and someone from the state will come out and investigate me. And that I can be punished for doing that."

Informing clients of their rights helps to establish a relationship of trust between the undocumented clients and the organization. When individuals know that their information is legally protected, they are often more willing to reveal sensitive information that could be important for their immigration case: "[Our clients] are able to provide information freely, because they trust that we're not going to share that information without their consent."

Academic institutions are bound by the Family Educational Rights and Privacy Act (FERPA), a law that safeguards student records. According to Seattle Community College Dreamers Support Navigator, "This law protects students because the institution can't share their private information, like the student's records." For them, FERPA is crucial to safeguarding the personal information of undocumented individuals collected by the college.

4.3. Leveraging technology for information security protection

All of the organizations we investigated leverage technology to protect the information of undocumented individuals. Currently, these measures include the use of

internal databases and listservs, data encryption, and several forms of electronic communication that are seen to have different levels of confidentiality.

WAISN uses encryption to ensure that the text messages sent over their reporting hotline and alert system are readable only by members of the listserv. WAISN technology team lead explains, "We do basic encryption, … we collect information through our hotlines between a SSL [Secure Sockets Layer] website and the login page."

NWIRP uses a web-based platform, LegalServer, to store client data, such as documents, forms that have been submitted to government agencies, and emails. This system is seen as an electronic backup to paper files. According to one of the legal advocate at the organization:

> "Whenever we submit [documents] to immigration, we scan everything into LegalServer, . . . in case the file is destroyed--you never know, like in a fire or whatever--so whatever happens we have it electronically as well."

This method allows for a secure transfer of information from the login screen into a remote server and database. The ECC leverages technology to safeguard the privacy of undocumented students who attend the many social and educational events at the Center. These events are open to all UW students and are widely photographed, the photos posted to Facebook, and attendees tagged by their friends, posing a security risk to undocumented students. The organization does have a low-tech method of helping the undocumented students avoid cameras—they are encouraged to wear large stickers as signal that they wish not to be photographed—but this system is, of course, not foolproof. As a safer method of preventing undocumented students from being identified on Facebook, the assistant director of the ECC teaches them how to adjust their Facebook settings so they cannot be tagged.

The administrative heads of both the ECC and LWB also leverage the perceived enhanced privacy of email, iMessage, and private Facebook groups over the publicly accessible Facebook pages. According to the Leadership without Borders coordinator, undocumented students most often choose iMessage and a private LWB Facebook page to communicate with herself and among each other. The students are not allowed to write posts on the public LWB page, nor are they encouraged to comment on the organization's posts. ECC assistant director draws finer distinctions between the levels of security of the various forms of electronic communication:

> "There are a lot of times we have to reach a lot of students, . . . so [we'll] try their emails, and they won't respond, and then we'll iMessage them and they'll respond right away… We'll try to get their attention on iMessage, and then if it's something a little more sensitive we'll try to keep it at least--so we have that trail on emails, which is more safe . . . I'll tell staff, if you have trouble you can get them through iMessage, but bring the conversation back to an email."

Both the interviewees work under the assumption that email represents the highest level of privacy, followed by iMessage, private Facebook pages, and public Facebook pages. However, according to lawyer and program director of the University of Washington Tech Policy Lab, the encryption protocols for iMessage do not preclude Apple from reading the content of these communications, and the company would likely cooperate with any subpoenas of text messages. Though iMessage privacy is currently

being decided in the courts, they do not consider this to be a safe mode of communication for undocumented students.

Current technology practice at the organizations we investigated is not without weaknesses, but at least one organization, WAISN, is considering options for future security enhancements. The Network is might soon move their sensitive data to overseas servers, possibly in Vietnam, where information could be stored beyond United States government jurisdiction. WAISN was also the only organization we contacted that was attempting to formulate strategies against hackers, especially as they begin to develop a mobile application for use by the undocumented. The team of volunteers at WAISN includes security specialists and hobbyists in technology. These experts are being guided by the THREAT model of security assessment, where systems managers assume the role of a hacker and try to capture any information that would be valuable from the data management system. As a final defense against hackers, WAISN might integrate a data "kill switch" into their data storage system, as a way to prevent the theft of information in an emergency situation.

4.4. Privacy self-management

Most of the organizations in our study discussed giving undocumented individuals the agency to make their own decision about the privacy of their information. Among the legal professionals we spoke to, several highlighted that although the organizations are the ones that send immigration applications to the government, the clients themselves must make the decision about whether or not to share specific information to the government. They highlighted that their clients can also dictate how information is stored within their organizations. When someone is not comfortable with their information being stored digitally, she keeps it only in their physical file. She also emphasized that the clients have the right to request copies of information about their case and store that information as they see fit, although she sometimes has concerns about risks they may be taking by inadvertently sharing this information.

Many of the nonprofit organization Facebook pages leave privacy decisions in the hands of the user. For example, in the case of a recent DACA information event at NWIRP, individuals had the option of selecting "attending" or "interested," which are visible to general Facebook users. Similarly, individuals can choose to leave personal testimonies in the form of reviews on both ICS's and NWIRP's Facebook pages.

Student groups on the University of Washington Campus also leave many decisions about sharing information to the students themselves. For LWB Coordinator, the student group's Facebook page is a place for members to "be open about their story as undocumented individuals, if they should wish to." Many students have chosen to "come out" as undocumented on the public Facebook page, posting their pictures, names, and personal immigration stories. They explain:

> "[The students] have been living with their undocumented status their whole life. They understand the risks better than anyone and don't need me telling them what they should or shouldn't share. If this is something that is important for them to do, for themselves, I'm not going to try to stop them. We don't do any policing here… A few students, a very small number (about 5 to 10 percent), choose to take on a more activist role and are open about their status. That is their decision to make, I am not going to try to stop them."

Though they view Facebook primarily as a platform for activism and peer support among the undocumented, they take a more protective stance towards the students when it comes to malicious comments posted by "conservatives and white supremacists" on the public LWB Facebook page. To avoid upsetting the students, they document and immediately delete such instances of hate speech.

Another example of privacy self-management at UW student organizations is the previously mentioned decision by the undocumented to wear stickers at ECC events, as a signal to others that they do not wish to be photographed.

4.5 Uniform privacy standards and training (or lack thereof)

Overall, of the nonprofits we interviewed none discussed a concrete set of information privacy standards or training provided to staff. For NWIRP legal advocate, privacy training in her office is "more as you go-- you just ask questions." They recall learning about certain practices like shredding information when it is no longer needed and keeping information confidential as some of the first standards she learned. The executive director of NWIRP stated that his recent privacy training is done through the requirements for grant making. Although one of the attorneys interviewed did not receive privacy training, her organization occasionally asks people to present about issues related to privacy as they come up. Some of those interviewed received training through other sources. For example, the technology director of WAISN states that workplace privacy training assisted him as a volunteer. ICS' lead attorney credits her knowledge of privacy training to a course she took on privacy law in law school. Data security and privacy standards are often left for third-party organizations that run the databases, such as LegalServer and the Immigration Law Group. In NWIRP's case, an internal IT department also addresses these issues.

Of the universities we spoke to, both Seattle Community College staff members received privacy training on FERPA, while the UW student organization leaders state they have received no training on privacy and security. "We've always just erred on the side of caution, especially with our students, anyways," states the assistant director of the ECC. He attempts to independently stay aware of current trends, discusses security strategies with the director of the campus queer student organization (from whom he got the idea of the no-photographs stickers), and passes that knowledge on to the students who help him manage social media. Similarly, the LWB coordinator explains: "I have not received any training. In general, I let the students take the lead in protecting their own security."

5. Conclusion

This study provides a preliminary understanding into the information practices and systems employed by humanitarian organizations to protect the privacy of the undocumented individuals they serve. Our research demonstrates gaps between current legal standards and best practices in technology found in the literature and the day-to-day functioning of these organizations, run as they are by often overworked volunteer staff. In response the rapidly changing political climate, some scholars have called for the need for security standards at nonprofits that assist the undocumented,

and are suggesting approaches to security audits at these humanitarian organizations (CHS Alliance, Groupe URD, & The Sphere Project, 2014; Greenwood, Howarth, Escudero Pool, Raymond, & Scarnecchia, 2017). This study responds to their call to survey current practices and the particular challenges faced by these organizations.

The staff of both nonprofit organizations and educational institutions spoke extensively about legal protections such as attorney-client privilege and FERPA, yet we found only limited awareness of data security. Additionally, we found very little in the way of concrete privacy standards and training, particularly in terms of digital privacy. In many cases, organizations are leaving complex, high-stakes decisions about the protection of personal information to the vulnerable undocumented individuals themselves. Given that members of this population often lack legal and technological sophistication, are struggling with poverty and inadequate health care because their access to many social services is blocked, and must deal with the fear of deportation and family separation, it should not be assumed that the they are in a position to manage their own privacy. The opinions of legal and information professionals that we encountered in the scholarly literature and in the process of conducting this research advise the most cautious approach to privacy management; we therefore believe humanitarian information organizations should take proactive efforts to protect the privacy of their vulnerable clients.

Our findings demonstrate the importance of providing support to humanitarian organizations in further developing standards and training for digital privacy. In many cases, these organizations struggle with limited budgets and capacity and would benefit from a set of shared guideline for the particular needs of humanitarian organizations working with undocumented migrants, which we hope further studies will address.

References

Cardia, I. V., Holzer, A., Xu, Y., Maitland, C., & Gillet, D. (2017). Towards a Principled Approach to Humanitarian Information and Communication Technology. *Proceedings of the Ninth International Conference on Information and Communication Technologies and Development*, 23:1–23:5. https://doi.org/10.1145/3136560.3136588

CHS Alliance, Groupe URD, & The Sphere Project. (2014). *Core Humanitarian Standard: Core Humanitarian Standard on Quality and Accountability*. Retrieved from https://corehumanitarianstandard.org/files/files/CoreHumanitarianStandard-English.pdf. (Links to an external site.)

Collier, A. (2017). Exploring Digital Sanctuary. Retrieved February 15, 2018, from OFFICE OF DIGITAL LEARNING website: https://digitallearning.middcreate.net/critical-digital-pedagogy/exploring-digital-sanctuary/

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

Ferguson, G. L. & S. (2006, May). The Framing of Immigration. Retrieved from Huffington Post website: https://www.huffingtonpost.com/george-lakoff-and-sam-ferguson/the-framing-of-immigratio_b_21320.html

Gildersleeve, R. E., Rumann, C., & Mondragón, R. (2010). Serving undocumented students: Current law and policy. *New Directions for Student Services*, *2010*(131), 5–18. https://doi.org/10.1002/ss.364

Gómez, R., & Vannini, S. (2015). *Fotohistorias: Participatory Photography and the Experience of Migration*. CreateSpace Independent Publishing Platform.

Gomez, R., & Vannini, S. (2017). Notions of Home and Sense of Belonging in the Context of Migration in a Journey Through Participatory Photography. *The Electronic Journal of Information Systems in Developing Countries*, *78*(0). Retrieved from http://www.ejisdc.org/ojs2/index.php/ejisdc/article/view/1763

Greenwood, F., Howarth, C., Escudero Pool, D., Raymond, N. A., & Scarnecchia, D. P. (2017). *The Signal Code: A Human Rights Approach to Information During Crisis*. Retrieved from https://hhi.harvard.edu/sites/default/files/publications/signalcode_final.pdf

Hollenhorst, O. (2017). *A rights-based evaluation of humanitarian information and communication technology policy* (M.A.). University of Washington, Seattle, WA.

Immigration Advocates Network, & Idealware. (2016). *Technology needs among immigrant rights and immigration legal services organizations*. Retrieved from https://www.immigrationadvocates.org/link.cfm?25937

Mangan, K. (2017). Why It's So Hard for Undocumented Students to 'Fix' Their Status. *The Chronicle of Higher Education.* Retrieved from https://www.chronicle.com/article/Why-It-s-So-Hard-for/239733

Marwick, A. E., & Boyd, D. (2018). Privacy at the Margins| Understanding Privacy at the Margins—Introduction. *International Journal of Communication*, *12*(0), 9.

Mendoza, S. (2016). *Giving Undocumented Students Safe Harbor on Campus*. *81*(5), 13–17.

Muhren, W. J., Eede, G. V. D., & Walle, B. V. de. (2009). Making Sense of Media Synchronicity in Humanitarian Crises. *IEEE Transactions on Professional Communication*, *52*(4), 377–397. https://doi.org/10.1109/TPC.2009.2032380

Muñoz, S. M. (2016). Undocumented and Unafraid: Understanding the Disclosure Management Process for Undocumented College Students and Graduates. *Journal of College Student Development*, *57*(6), 715–729. https://doi.org/10.1353/csd.2016.0070

National Immigration Law Center. (2017a). New Questions and Answers About DACA Now That Trump Is President. Retrieved February 15, 2018, from National Immigration Law Center website: https://www.nilc.org/issues/daca/daca-after-trump-q-and-a/

National Immigration Law Center. (2017b). Understanding Trump's Executive Order Affecting Deportations & "Sanctuary" Cities. Retrieved February 15, 2018, from National Immigration Law Center website: https://www.nilc.org/issues/immigration-enforcement/exec-order-deportations-sanctuary-cities/

Newell, B. C., Gomez, R., & Guajardo, V. E. (2016). Information seeking, technology use, and vulnerability among migrants at the United States–Mexico border. *The Information Society*, *32*(3), 176–191. https://doi.org/10.1080/01972243.2016.1153013

Norris-Tirrell, D. (2014). The changing role of private, nonprofit organizations in the development and delivery of human services in the United States. *Journal of Health and Human Services Administration*, *37*(3), 304–326.

Olijnyk, N. V. (2015). A Quantitative Examination of the Intellectual Profile and Evolution of Information Security from 1965 to 2015. *Scientometrics*, *105*(2), 883–904. https://doi.org/10.1007/s11192-015-1708-1

Olivas, M. A. (2010). Enrolling Undocumented Students: FAQs. *Recruitment and Retention in Higher Education*, *24*(9), 3–4.

Raymond, N., Al Achkar, Z., Verhulst, S., Berens, J., & Barajas, L. (2016). *Building data responsibility into humanitarian action* (No. 18; pp. 1–15). Retrieved from OCHA - United Nations Office for the Coordination of Humanitarian Affairs website: http://www.unocha.org/sites/dms/Documents/TB18_Data%20Responsibility_Online.pdf

Ritvo, D. T. (2016). *Privacy and Student Data: An Overview of Federal Laws Impacting Student Information Collected Through Networked Technologies*. Retrieved from https://dash.harvard.edu/handle/1/27410234

Solove, D. J. (2013). Introduction: Privacy Self-Management and the Consent Dilemma. *Harvard Law Review*, *126*(7), 1880–1903.

Vannini, S., Gomez, R., & Guajardo, V. (2016). *Security and Activism: Using participatory photography to elicit perceptions of Information and Authority among Hispanic migrants in the U.S.* Presented at the iConference, Philadelphia, PA, USA.

Vannini, S., Gomez, R., & Newell, B. C. (2019). *Documenting the Undocumented: Privacy and Security Guidelines for Humanitarian Work with Irregular Migrants*. Presented at the iConference 2019, Washington, D.C.