Keeping a Low Profile? Technology, Risk and Privacy among Undocumented Immigrants

Tamy Guberek,[1] **Allison McDonald,**[2] **Sylvia Simioni,**[1] **Abraham H. Mhaidli,**[1]
Kentaro Toyama,[1] **Florian Schaub**[1,2]

[1]School of Information
University of Michigan
Ann Arbor, MI, USA

[2]Computer Science & Engineering
University of Michigan
Ann Arbor, MI, USA

{tamyg, amcdon, ssimioni, mhaidli, toyama, fschaub}@umich.edu

ABSTRACT

Undocumented immigrants in the United States face risks of discrimination, surveillance, and deportation. We investigate their technology use, risk perceptions, and protective strategies relating to their vulnerability. Through semi-structured interviews with Latinx undocumented immigrants, we find that while participants act to address offline threats, this vigilance does not translate to their online activities. Their technology use is shaped by needs and benefits rather than risk perceptions. While our participants are concerned about identity theft and privacy generally, and some raise concerns about online harassment, their understanding of government surveillance risks is vague and met with resignation. We identify tensions among self-expression, group privacy, and self-censorship related to their immigration status, as well as strong trust in service providers. Our findings have implications for digital literacy education, privacy and security interfaces, and technology design in general. Even minor design decisions can substantially affect exposure risks and well-being for such vulnerable communities.

ACM Classification Keywords

H.5.m. Information Interfaces and Presentation (e.g. HCI): Miscellaneous; K.4.2 Computers and Society: Social Issues.

Author Keywords

Technology use; privacy; online risk; surveillance; undocumented immigrants; immigration; integration.

INTRODUCTION

Like almost everyone else today, undocumented immigrants are users of information and communication technology (ICT). While ICTs have been found to support immigrants' integration in new contexts [27, 28, 31, 94], technology can also enable discrimination, harassment, and government surveillance, the latter potentially leading to devastating consequences such as detention, deportation, and family disruption. For the estimated 11.3 million undocumented immigrants in the United States [72], these risks have intensified recently due to increased immigration enforcement and anti-immigrant sentiment [53, 54, 58].

Little is known about what role technology plays in the daily lives of undocumented immigrants and how it affects their vulnerability. Undocumented immigrants would be expected to have strong motivation to protect their privacy when using technology [30, 59, 87], but it is unclear how aware they are of ICT-related privacy and surveillance risks, whether they adopt privacy-protective strategies, or how effective any such strategies are. Prior research on online privacy behavior of the general population suggests that, despite concerns, people often do not take protective action [50, 95].

To understand how undocumented immigrants navigate the benefits and risks of digital technology, we conducted semi-structured interviews with 17 Latinx[1] undocumented immigrants in an urban U.S. Midwest context. Undocumented immigrants from Latin America constitute the largest such group in the United States [72].

Our findings provide new insights on undocumented immigrants' technology use practices, as well as their understanding and attitudes toward digital security and privacy. To a great extent, our participants' behaviors with respect to security and privacy reflect that of the broader population — despite some concerns, they were neither particularly concerned about online privacy, nor did they take significant steps to protect it. This is surprising given the far greater threat that information disclosures have on their lives. We identify a number of reasons for this: First, smartphones and social media are viewed to have indispensable benefits by our participants. Second, our participants have only a vague understanding of technology-related privacy and surveillance risks, making any potential

[1]Latinx is a gender-neutral term referring to both Latinos and Latinas.

CHI 2018 April 21–26, 2018, Montreal, QC, Canada

ACM ISBN 978-1-4503-5620-6/18/04.

DOI: https://doi.org/10.1145/3173574.3173688

consequences seem uncertain. Third, they tend to place significant trust in the major social media platforms. Fourth, participants feel that any information about them is readily available to government authorities, so they did not think *additional* exposure online would affect that risk.

These findings have implications for the development of educational resources for the immigrant community; the design of transparency cues and privacy controls; and the design of ICTs in general. Even minor design decisions, such as the use of phone numbers as account identifiers, can substantially affect the exposure risk of vulnerable communities.

RELATED WORK

To situate our research, we describe related work on integration of undocumented immigrants, immigrants' technology use, and research on privacy and security concerns and behavior.

Undocumented Immigrants and Integration

Prior research has studied many challenges undocumented immigrants face [45], including cultural integration [10, 25], health [60, 70], and parenting [88]. Children of undocumented immigrants, even if they have legal status, struggle with identity, isolation, stress and anxiety [23, 44, 48], as well as reduced political integration [20].

One way undocumented immigrants avoid risks that come with their vulnerable legal status is to limit contact with authorities and institutions, even non-governmental ones offering heath care and social services [10, 25, 60]. They may also limit, or even avoid, going to public places such as supermarkets, parks, and cultural events [49, 60]. However, immigrant families also demonstrate resilience. Immigrants form new networks [42, 66]; families stay in touch with relatives abroad [25, 75]; and youth adapt quickly through peer interactions and formal education [37, 86]. A prominent theme in this literature is intergenerational dynamics, such as children's roles as interpreters and mediators for their family members [78, 105], or their wrestling with social identities [12, 25, 37, 78].

Immigrants' Technology Use

How immigrants around the world utilize ICTs in their day-to-day lives has been studied extensively, showcasing a community of people who actively engage in technology for a wide range of purposes. Studies have found that immigrants rely heavily on mobile phones [39] and that ICTs not only help immigrants communicate with those back home, but also aid their integration into new societies [22, 27, 28, 31, 94].

Less research has focused on technology use by undocumented immigrants in the United States, but the existing prior work echoes findings of ICT use among other immigrant populations. Undocumented immigrants use ICTs (primarily mobile phones) to enhance their integration experience (e.g., to find jobs) and to stay in touch with family abroad [8, 9]. Undocumented youth use social media in creative ways to contribute to social movements and to fight for their rights [30]. Gomez and Vannini [43] find differing behavior among undocumented populations attempting to cross the border and those who have already settled in the U.S. And, while Constanza-Chock notes that privacy and security concerns about technology are especially salient for immigrants [30], little is known about how technology risks are perceived by undocumented immigrants living long-term in the United States.

Privacy and Security Concerns and Behavior

We live in a world of mass surveillance and unprecedented personal data collection, as evidenced by the Snowden NSA leaks [46], targeted advertising [106], vast quantities of online personal sharing [40], and the digital traces left by everyday activities [80].

Online privacy and disclosure risks on social media, as well as strategies for navigating them, have been studied extensively [36, 51, 97]. People use diverse strategies for managing self-disclosure. Individuals also have to navigate networked privacy and group privacy issues [32, 87], including tensions that arise from "boundary turbulence" [73], i.e., how information about you can be disclosed by others [6, 13, 56, 73]. Lampinen et al. distinguish among three dimensions through which people manage boundary turbulence in social media: preventative and corrective strategies; mental and behavioral strategies; and individual and collaborative strategies [56].

Yet, research on online privacy and privacy behavior suggests that overall, people often do not take protective action [50, 95]. Known as the "privacy paradox" [7, 69], individuals struggle to translate intentions to protect their privacy into action, often sharing potentially compromising information about themselves [47] and regretting it later [100]. Reasons for the privacy paradox include bounded rationality in privacy decision making [2, 3, 74], misconceptions about information flows [5, 55, 57, 77, 82], misconceptions of protective measures [52, 76], and context violations [59, 68]. These issues are exacerbated when people are unaware of the risks involved, or do not fully understand their implications. More generally, Slovic finds that unknown risks are perceived as less dangerous [84]. Furthermore, when technology risks are uncertain, studies have found that trust in companies and platforms serves as a key heuristic in guiding people to override potential concerns [64]. Other studies have focused on marginal risk perceptions, and found that if personal information may otherwise be public, individuals will invest less in protecting it themselves [4].

Companies may exploit decision heuristics to nudge users towards disclosing more information [2, 3, 16]; affordances of social media platforms have been shown to strongly influence users' self-disclosure behaviors [6, 24, 97]. Options for alternate platforms or encrypted communication channels are limited; while security and privacy tools like anonymous browsing [35], decentralized social networking [34, 62], and encrypted communication tools [15, 107] are active research topics, these tools have not been widely adopted. Many studies have uncovered hurdles and usability issues in adopting new security or privacy tools [1, 41, 102].

There is some research on privacy and security behavior of specific vulnerable communities, including teenagers [17], journalists [65], recovering addicts [104], intimate partner abuse survivors [63], parents of LGBT children [14], home-

less populations in the U.S. [103], and urban populations in the developing world [26]. These studies reveal nuanced, community-specific concerns and practices. A recent population survey [61] found that many people of low socioeconomic status (SES) in the United States are acutely aware of digital harms, feel "very concerned" about digital privacy and security, and display low trust in Internet-service providers. The study also finds that low-SES Hispanic adults are most sensitive to privacy risks, know of few resources to protect themselves, but express high interest in learning how to do so. Studying Muslim-Americans, Sidhu found that despite widespread belief that their online activities were monitored by the U.S. government, few altered their online behavior to address these concerns [83]. Overall, there is no blanket theme that all marginalized communities have in common regarding privacy practices. Privacy risks are varied, diverse, and differ among populations given their individual status and place in society.

Our study contributes to the literature by considering technology issues among an especially vulnerable community, Latinx undocumented immigrants in the United States.

BACKGROUND

Threats to undocumented immigrants have intensified recently in the United States [58], where immigration enforcement is in the purview of the Immigration and Customs Enforcement Agency (ICE). ICE already grew substantially under the Obama Administration, with the Trump Administration planning to add 10,000 more ICE officers [67, 90].

ICE has also expanded its technical capabilities. Today, individuals stopped by ICE will typically have their fingerprints scanned, even without arrest [11]. Facial recognition is becoming prevalent: in 2016, Customs and Border Patrol (CBP) solicited proposals for consumer-sized drones equipped for facial recognition and cross-referencing with law enforcement databases [19]. In January 2017, President Trump called to expedite biometric data collection at all ports of entry [92].

Meanwhile, privacy protections for immigrants are being eroded. In 2017, President Trump issued an Executive Order on "Enhancing Public Safety" that removed all protections of the Privacy Act for undocumented residents, thus expanding data sharing between federal agencies [11, 91]. In Vermont, the Department of Motor Vehicles has allegedly been responding to information requests by ICE and other federal agencies by running facial recognition against their state ID database, in violation of its own state law [89]. Concerns over data sharing have been renewed with the recent termination of the Deferred Action for Childhood Arrivals (DACA) program for undocumented immigrants who arrived in the U.S. before the age of 16. DACA granted registrants work permits, drivers' licenses, and a renewable two-year stay of deportation [33]. Post-DACA, how information about DACA registrants will be used is unclear.

How ICE currently uses social media data is not well-documented, but its use seems to be increasing. In September 2017, the Department of Homeland Security published their policy of collecting social media handles of all immigrants, including permanent residents and naturalized citizens [38, 98]. In 2017, ICE officers in Detroit submitted a warrant to Facebook to collect the phone number of an undocumented man. His phone number was then used to locate him by tracking his mobile phone with a cell-site simulator (known as a "Stingray" device) [85].

STUDY DESIGN

Between July and September 2017, we conducted 17 interviews with Latinx undocumented immigrants (14 women, 3 men) in an urban area in the U.S. Midwest. These were conducted in-person at a participant's home or in spaces trusted by them (e.g., a church or restaurant). Sixteen interviews were conducted in Spanish by at least one of the native Spanish-speaking co-authors; one was in English. The interviews were audio-recorded and lasted 66 minutes on average, ranging from 52 to 81 minutes.

Before reaching out to potential participants, we spent several months developing relationships with local immigrant rights organizations and community allies to assess how we could best recruit undocumented persons while protecting their privacy. Several allies then distributed advertisements for our study through their networks. Despite going through these trusted channels, recruitment was slow initially. After a first few participants, we were able to reach the other participants via snowball sampling, but even then, we had to follow up repeatedly with potential participants. Especially among men, we faced considerable difficulty in recruitment.

Interview Themes and Protocol

We developed our semi-structured interview protocol through iterative literature review and conversations with allies of the immigrant community.

In order not to be suggestive of sensitive issues, we began all interviews (as well as recruiting) by focusing on technology use in general, avoiding mention of privacy, security or surveillance. We asked about participants' daily lives, community activities, and immigration stories. We then asked them to describe their daily technology use: which devices and platforms do they use, how frequently, and for what activities. We asked participants about frustrations or concerns with the way they use technology. If it did not come up naturally, we then asked whether they had concerns about technology given the broader challenges of the undocumented community. Then, we asked about their privacy and security practices online, eventually probing about security tools, privacy settings, password practices, etc. Finally, we invited them to share any final thoughts or concerns about technology. Demographic data was collected after the interview via a questionnaire.

Participants received $20 for their participation. The study was exempted by our IRB, and documentation requirements regarding payments were waived in order to ensure participant privacy.

Data Security, Coding and Analysis

We followed a strict security protocol in handling participant data. Audio files were encrypted before storing them in our

institution's cloud storage, which is certified for sensitive identifiable human subjects data. No unencrypted documents contained identifying information for any participants. Furthermore, we did not discuss sensitive content about our interviews or participants over email.

All interviews were transcribed and translated by bilingual research team members; for the first eight interviews, one Spanish-speaking team member transcribed the Spanish audio recording, then translated the text to English. A second Spanish-speaking co-author spot-reviewed the English translations against the audio recordings. Because quality was high, we translated the remaining nine interviews from Spanish audio recordings directly into English transcripts. Again, a second co-author spot-reviewed the translated English transcripts. All potentially identifying information was redacted in the transcription process.

Qualitative analysis was conducted on the redacted, English transcripts. We used an inductive coding process and thematic analysis. Two of the interviewers identified preliminary themes, which were developed into an initial codebook. Through multiple iterations of independently coding different interviews, each followed by collaboratively revising the codebook, we arrived at a stable codebook with good interrater reliability (Scott's Π=.692). One researcher then coded the remaining interviews and recoded the interviews used for codebook development. Using thematic analysis, we explored the 80 codes grouped by overarching categories to identify and analyze prevalent themes.

PARTICIPANT POPULATION

Despite our best efforts to seek participants with diversity in age, gender, and occupation, our sample (see Table 1) was dominated by women with children (76%) in their thirties and forties (median 38). They are settled immigrants, the majority from Mexico (88%), who have been in the United States 10–17 years (median 14). Most are part of mixed-status families, with children 1–30 years old. Some have children they brought with them into the United States (29%), but most have U.S.-born children (88%) who are therefore U.S. citizens. The prolonged stay in the U.S., and the establishment of mixed-status families, is typical of the broader undocumented immigrant population in the United States [45].

Most participants told us about their journey to the United States. At least two reported arriving by plane and overstaying their travel visas. Most others traversed the U.S.-Mexico border by foot under rough conditions, lacking food and water, and then taking collective vehicles to their final destination. Experiences ranged from taking eight days to up to two months to cross from origin to destination. Most successfully arrived as desired, but a few arrived only after multiple attempts.

Limitations

Gender and place of residence, among other variables, can substantially shape undocumented immigrants' experience of illegality and integration [29, 45, 71]. Our participants were mostly women who all had been in the United States for over 10 years. Undocumented men, individuals who only recently entered the country, as well as undocumented immigrants in other areas, especially close to the border, may exhibit other technology use patterns or risk perceptions. Furthermore, research with "hidden populations" is challenging. Our sample is small and should not be construed as representative. Instead our research was exploratory and provides initial insight into technology's role for undocumented immigrants.

ID	*Gender*	*Age*	*Origin*
P1	F	40-44	Mexico
P2	F	40-44	Mexico
P3	F	30-34	Mexico
P4	F	30-34	Mexico
P5	M	40-44	Mexico
P6	F	40-44	Mexico
P7	F	40-44	Mexico
P8	F	30-34	Mexico
P9	F	30-34	Mexico
P10	F	40-44	Mexico
P11	M	35-39	Mexico
P12	F	35-39	Costa Rica
P13	F	30-34	Mexico
P14	F	18-20	Mexico
P15	F	50+	El Salvador
P16	M	30-34	Mexico
P17	F	35-39	Mexico

Table 1. Participant demographics.

FINDINGS

Below, we go through our findings in three broad categories: daily offline life as it pertains to immigrant status; general digital technology use; and issues related to privacy and security.

Navigating Risks in Daily Lives Offline

Most of our participants spoke proudly about how well they have integrated into their local communities and their efforts to live as "normally" as possible. Trusted places such as schools, churches and public libraries serve as safe spaces. Nevertheless, there is a fragility to their life, not only due to the ever-present threat of immigration enforcement, but also due to the reliance on good will of employers, local authorities, neighbors and others. Some go to great lengths to protect themselves while others try to avoid constantly thinking about risks. The recent intensification of immigration enforcement has also strengthened many of our participants' commitment to helping other community members protect themselves by sharing relevant information with them.

Fears of detention and deportation

The lack of "papers" loomed large for our participants. They expressed a sophisticated understanding of their risks due to lack of legal status. Most mentioned that immigration authorities could show up to detain and deport them at any time, with devastating effects. P12 shared a respective experience: *"They asked [my neighbor] if there were more Hispanics [...] that did not have papers. So, they are not truly looking for anyone in particular. They are just searching for someone to take. [...] I was really nervous and got this huge headache, and I*

thought, 'My son is inside and if they come and take me, what will happen to him?' ICE was there all week, so we had to be careful about going outside."

About half of our participants tried to avoid thinking about their risks constantly, whereas the other half made significant adjustments, as discussed below.

Limiting exposure to authorities

Many participants have had direct contact with authorities at various levels (federal, state, local) for issues related to paying taxes, addressing traffic violations, or applying for privileges for their U.S.-born children (e.g., single custody or food stamps). Therefore, they perceive that at some level, authorities already have some of their personal information. Others actively tried to avoid providing information to authorities, even when it meant opting out of potential benefits: *"We've delayed ourselves in getting DACA for our son. It's due now. Lately, when you go and fill out the application, supposedly it's supposed to be confidential, that just your children's information will be on it. But I've heard that they ask for the rent agreement, and we're all on that. There are names, our address, the phones"* (P10).

Driving was frequently mentioned, given that the participants' state no longer issues driver's licenses to undocumented immigrants. Being stopped for traffic violations is mentioned by many as a risky scenario that could lead to greater problems (a finding echoed in prior work [49]). Yet most participants risk driving even with concerns. P11 said *"I drive calmly. I know what can happen, but I try not to think about it."* A few participants have chosen not to drive at all. P10 explained, *"The truth is, I never learned to drive for that reason, because the police would detain me."* While P15 has been driving during her 15 years in the United States, she stated that recent intensification of immigration enforcement led to greater fear when she was on the road.

Risks from information disclosures to authorities by others

Two participants mentioned experiences where disclosures by people they knew led to immigration authorities locating them (P14, P16). For example, *"Immigration had gone to my cousin's house and he had a brother who told them I was their cousin in addition to where I worked [...] We try to be careful all the time, but sometimes the problem is not us but other people"* (P16). But for these two participants, the information disclosures did not lead to greater care with their information — there was a feeling that the authorities already knew what they needed to pursue enforcement actions.

Intensification of perceived risk

Almost all participants emphasized a mounting sense of risk since the U.S. presidential election in November 2016. In response, participants reported making inconvenient adjustments in their daily activities. P10 recounted how she and her husband no longer leave their child home alone: *"[My daughter] has to get up earlier so [my husband] can take her, because we cannot leave her alone, because we do not know what is going to happen."*

Similarly, P12 said, *"Now we have to be more careful, even in the stores. One sees that they look at you badly, so I'd rather avoid those things. I even avoid talking in Spanish, so I talk to my son in English instead."* She mentioned that many in her community have recently prepared documentation to facilitate child custody in case they were arrested.

Most participants also referenced increased harassment, racism and social stigma in interpersonal interactions over the past year. Many participants felt that strangers are now more open with anti-immigrant sentiments. P12 recounts: *"I was at the pharmacy and my son was talking to me in Spanish, so there was a lady who got mad and told the cashier that they should only allow people who speak English."* Another negative experience was shared by P10: *"My sister-in-law told me a few days ago that she went to a park and saw a woman who asked her, 'Where do you work? That's a nice uniform. Do you clean houses? Where is your permit?' And, very ingenuously, she replied, 'I don't have one.' The lady then said Trump was going to take all the Latinos out. It's ugly."*

Perceived obligation to share and inform others

Along with the increased sense of insecurity, almost half of our participants mentioned a growing sense of collective identity with other immigrant families over the past year. Technology is increasingly used to share information about the presence of immigration officers, news of raids, or any other immigration enforcement related activities. P1 noted, *"One feels more responsibility in passing on this information."* Such distribution of information was also perceived by participants as an opportunity to regain some autonomy and sense of empowerment.

Undocumented Immigrants' Technology Use

Technology plays an essential role in our participants' lives. All participants used smartphones, with usage dominated by communication with friends, family, and community institutions through apps such as Facebook and WhatsApp.

ICT adoption driven by communication and convenience

For many participants, ICTs are indispensable. For example, banking, scheduling doctor's appointments, and receiving information from the schools their children attend, such as grades and absences, are all done online. P11 explained: *"From the school, it comes to my email, so everything goes there directly. When I go to the appointments, it's on my email."* These needs (and how it was often inconvenient to navigate these daily activities without ICTs) were driving factors behind the adoption of some technologies, such as email.

ICTs are also instrumental for communicating with friends and family back home, and in many cases, newer technologies offer significant convenience. P15 stated: *"Before, I needed to buy [international calling] cards at the store. Thunder, raining, or lightning, I had to get these cards. Sometimes I would buy the $25 cards and never use them, but when I did, I would have no balance left.... That's why [Facebook] Messenger is a perfect technology, because with it I can talk to my daughters and see my mother."*

Family also played a role in technology adoption. For some participants, family members were the ones advising and encouraging the use of technology. A few participants described how information (such as Facebook passwords) was managed

by a family member. Many participants were also motivated by their roles as parents to develop their competency with technology: most expressed a desire to become comfortable with general computer tasks, and expressed concern over their limited ability to assist with homework and prevent their children's exposure to cyberbullying or adult content.

Mobile-primary lifestyle

Although many participants own both computers and tablets in addition to mobile phones, all participants use their smartphone as their primary device. A few of our participants also noted that they depended solely on their mobile data for access to the Internet. Convenience and ease-of-use were cited as reasons for this mobile-primary lifestyle. P3 works as a housekeeper: *"In the work I do, everything is now by text, because I no longer answer calls since I'm on the job cleaning with another person. [...] I check how [my daughters] are, to see if they've eaten. With my husband, I use it to look up directions. I even use it to know how to cook turkey."*

The central role of Facebook

All but one participant were active Facebook users. Main uses were keeping in touch with friends and family abroad; engaging in their local community; and finding events in their area. WhatsApp was the second most-used tool; primarily used for video calling, voice messaging, and photo sharing with family abroad. Facebook Messenger was used in largely the same way, although mentioned less. A few participants mentioned other tools, such as Instagram, Snapchat, and Twitter, but most comments regarding social media revolved around Facebook, WhatsApp, and Facebook Messenger. All but one participant had Facebook accounts and all but three had WhatsApp accounts. This indicates a heavy reliance on a small and consistent set of tools — notably, all of which belong to a single company: Facebook.

Adoption of tools is motivated by ease of use and people in their networks using them. P12 says *"The only thing I use is Facebook and WhatsApp, because they're the easiest and other apps are too heavy."* When deciding on creating a group for their community, P1 said *"So I did some research and decided on WhatsApp. Everyone has it and it's free, so I downloaded it and added everyone."*

Risk Perceptions and Mitigation in Technology Use

While participants were mostly enthusiastic about the benefits of technology, they reported a range of risks — from common security and privacy concerns unrelated to their legal status to various kinds of unwanted visibility that could lead to more extreme consequences. While participants sought privacy and safe spaces for intimate communication through "network regulation" [97] and careful self-disclosure, channel choice, and a degree of self-censorship on social media, most participants expressed resignation with respect to the risk of immigration-related surveillance.

Common privacy and security concerns

Asked about concerns and perceived risks of technology use, most mentioned security-related threats that are not unique to their immigration status — concerns such as identity theft, online financial fraud, unauthorized access to their Facebook accounts, and hackers who might steal their information or impersonate them online. Some also brought up concerns with strangers watching or contacting their children online, and with children harassing and bullying each other through technology. For the most part, technology-related risks regarding their status were not at the top of our participants' minds.

Valuing privacy and intimacy

Many participants mentioned a general desire for personal privacy, without explicitly relating it to their immigration status. This desire came up most prominently with respect to social media, especially Facebook. While everyone highlighted the benefits of Facebook, most noted a desire for "intimate interaction," especially with family abroad.

With respect to these concerns, participants saw their privacy and security as largely being in their own hands. Almost all participants reported expending effort on network regulation, curating an intimate network of people to maintain Facebook as a safe space for them. They have restrictive friending practices (*"only friends and family"*): *"I am very selective about social media. I have people who I really know and people I know from far away. I only have family and nearby friends, but besides that, no"* (P3).

Participants also expressed concerns about strangers contacting them: *"There are people we don't know and send invitations as if they were friends. I don't accept just any person if I don't know them. I have a lot of requests but I don't accept them because I don't know them. I only accept those I do know and talk to both here and in Mexico"* (P7).

Two exceptions were participants who mentioned that their network included mostly people who they know but with whom they have looser ties, or even distrust. Given context collapse concerns, they mostly abstained from posting on Facebook to avoid creating windows into their lives.

Overall, most participants displayed trust and confidence towards people included in their curated network, and talked about Facebook as an intimate, safe space.

Limiting self-disclosure

While most people regulate their network to keep it intimate, the way participants stated their privacy goals also reveals a deeper sense of concern about unwanted disclosures.

Concerns with photos came up most often. Some participants were happy to post pictures and saw this as an enriching aspect of keeping in touch with family abroad. These participants varied in terms of how they shared photos within Facebook. Half were happy to post intimate content in their profiles, whereas the other half were more cautious. Some of them rarely posted pictures of themselves on their profile pages, and if they did, made sure not to reveal locations or intimate spaces. For example, P12 explained: *"I don't like having everyone see my Facebook. Just people who know me that I interact with. There are photos of my son and friends. I do it overall for my son, because I don't want people knowing where I live, [...] if we're somewhere else, fine. But my house or anything showing my house number, no."*

Specifics about the consequences of disclosures were rarely elaborated on. Only P4 specifically expressed that posting location information could result in physical safety risks: *"The majority of people who use social media, they post their location all the time or where they are, but one doesn't know that someone might come and do something. So, that's my worry, that someone knows where I'm going and tries to harm my family. I'd rather abstain."*

Some only shared photos privately, i.e., one-to-one or in small groups via Facebook Messenger. More broadly, we observed systematic selectivity between spaces/channels offered within Facebook, and the public/private notions about each of these. Participants tended to view profiles as the most public place within Facebook. They viewed Facebook Messenger as the most private channel, where those with reservations about unwanted disclosures are more likely to share intimate content with trusted individuals and groups. WhatsApp was not considered part of Facebook. When asked about preferred communication channels, one participant had a sophisticated notion of WhatsApp's security: *"WhatsApp is more private than Facebook ... because it's encrypted and had other features that other apps don't have. It has more privacy"* (P5).

Some of the perceived risks were tightly bound to participants' home country, but separate from immigration status. Specifically, many of our participants come from regions in Mexico where kidnappings, extortion and physical violence are common. Two participants shared anecdotes about perpetrators using location information from social media in kidnappings back home. P16 worried that details about his lifestyle in the U.S. could be interpreted as affluence and put family members back in Mexico at risk of extortion: *"The problem is that if one posts them, there will be people in Mexico who will see them and think that since one is here, one has enough money and they'd want to do something bad to other family members."*

Many participants raised concerns about participating in digital public spaces. Several people mentioned online harassment, which they credited to a more openly xenophobic atmosphere in the U.S. since Fall 2016. P1 stated: *"There was a link about political topics on [a local news website] and the boy commented on it and there all these racist people came to attack. It reached the point where they quickly found his profile and even where he lived, and they threatened with sending immigration [enforcement] to his family."*

Participants tried to avoid such risks by not engaging in online public discussions. For example, P3 said: *"On social media, I've seen lots of things about people being taken away by ICE. It got me angry seeing reports on the news, because you start to see the comments, and I feel a lot of impotence ... you think and you don't comment back. Mostly, you get upset and you stay that way, because I hear about a lot of people who are afraid for their kids or of being followed and all that."*

However, in digital spaces perceived to be public, some participants opt for more open sharing of their political or social views, although this could sometimes create tensions. For example, P14's view on expressing her political opinion on her Facebook profile differed from her mother's: *"My mom now has been [saying] 'I don't think you should share that, [...] cause when immigration investigates you and they see that, they're not gonna want to give you your papers because you don't like their president.' [I said,] 'Listen, I'll share my thoughts before I get any papers.' "* This situation is indicative of the strains undocumented immigrants in the current socio-political context have to navigate, and the looming sense of resignation that all content can potentially be surveilled and investigated.

Overall, participants primarily managed privacy and security concerns through a limited set of practices: network regulation, varying degrees of self-censorship and deliberate choice of communication channels.

While self-disclosure was the main privacy-related concern mentioned, it was not the only source of stress — just being connected to information networks could be taxing. More active social media users among our participants noted that too much information related to undocumented immigrant issues, such as raids or deportations, weighs heavy on them. While they valued rich information sharing and mentioned technology as a channel for receiving support, they were concerned about effects of information overload on themselves and family members. P2 stated, *"Sometimes it's good to have support from the community, but sometimes it's bad because to be constantly reading this kind of information, it's exhausting. And this is through whatever means of communication, so much as in television, radio — it's all the same. And it's too much."*

Concerns about disclosures by others

For undocumented immigrants, privacy takes on a collective character in various ways, with implications for shared responsibility within family units, other undocumented immigrants in their networks, and allies. Others can deliberately or inadvertently disclose information about undocumented individuals or groups via technology in various ways, creating privacy "boundary turbulence" [73] and potentially putting those individuals at risk. Yet, most of our participants did not perceive these as concerns. To the contrary, most only expressed their appreciation for social media groups that were used for immigrant-related information sharing and coordination. Several of these groups have formed in response to increased immigration enforcement risks. Only P2 expressed concern of being associated with such groups. She worried that group members' identifying information could end up in the wrong hands if one of them would be arrested or detained: *"One of the young men they detained was part of the group, so I got worried and thought, if they're checking everyone's social media and they find the group, well, they can find me and that's that."*

Concerns about being exposed affected participants' engagement in community activities. Some participants regularly attend events related to undocumented immigrants, such as vigils, informational sessions, or local government public forums debating these issues. A few of these participants were beginning to question the risks of doing so. A few wondered out loud whether they should be concerned with the relative ease with which events in the physical world can leave digital

traces, as information, such as photos, could move easily from meetings in physical safe spaces to more public online spaces. These participants raised how important it was that organizers and other attendees were conscientious about protecting undocumented attendees. They sensed a lack of autonomy and control over their information, but they also felt uncertain about the extent to which they were exposed to respective risks. P2 talked about a photo of her taken at an event continuing to circulate and reappear in perpetuity: *"... every time that topic is discussed, my picture shows up [laughs]."* For a few other participants, the risks of exposure related to attending events, was simply seen as too high — although not specifically due to the ways in which technology may exacerbate the risk. They simply avoided immigrant-specific events completely. P3 stated: *"the more you hide, the less you have to fear."*

Trust in platform providers

Some participants expressed discomfort with how certain platforms reveal information about them, but in general participants expressed trust in the platforms they use. In response to questions about their conceptions of any adversaries in their technology use, none seemed to consider the service provider as an entity that had access to their data. In fact, the overwhelming attitude was that service providers such as Facebook were looking out for the users' best interests by alerting them if they had a suspicious login attempt or by providing privacy settings that allowed them to control who could see their content. Conversely, although several participants had negative experiences with social media platforms not working as expected, none of the experiences garnered significant frustration or anger directed toward the company. In one example, P14 found that Snapchat was sharing her location with all her friends without her knowledge. When she discovered this, she changed the location permissions on the app and continued to use it, expressing only surprise and confusion as to why Snapchat would suddenly make such information visible. Despite Snapchat's violating her privacy through opaque feature changes, P14 did not express any direct criticism of Snapchat.

Exceptions to the general trust in platforms were expressed by a few participants who noted that WhatsApp shared identifying information with other users in group chats, especially people who are outside their phone contacts. This may include phone number, profile photo, name, and their online status, depending on privacy settings. For instance, P13 felt very uncomfortable that her ex-partner was able to keep track of her, in her words, *"because on WhatsApp, it says when you're online;"* a known privacy issue [21]. Another participant disliked how WhatsApp enabled one of her contacts to add her to a group with others she does not know. She felt that this created uncomfortable encounters and was an invasion of her privacy, so she stopped using WhatsApp entirely. However, opting out like this was the exception among our participants.

Overall, participants who had negative experiences with technology did not hold the companies accountable, but were generally quick to give credit to services that allowed them to manage interpersonal risks, such as unwanted access to information by others and account compromise. Considering that large technology companies have acquiesced to government requests for private information, this view that risks just stem from users, not from the tool (e.g., through warrants or data aggregation across tools), could be problematic.

Surveillance concerns and resignation

Throughout, many participants expressed some notions of surveillance, primarily in the form of concerns with "others" having unauthorized visibility of them or their families. This concern is mentioned across technologies, from TVs, social media, messengers, to technology in general. While participants are mindful of which information they share on public Facebook pages or through Facebook Messenger and WhatsApp, there is nevertheless a sense of an omnipresent threat of surveillance by all-encompassing "others" in both public and private areas of the tools they use. For example, P12 says of immigration-related content, *"many people feel afraid of that information showing up on their page and think someone might be watching."*

Five of our participants brought up the specific concern that "the government" has the power to track, observe, and gain access to information about members of the community via technology. For example, P14 stated: *"It's so scary to see that immigration [enforcement] checks everything about you. I mean, you have no privacy. My Facebook could be private, but they could probably see it. They could probably hack into my messages. They could probably do anything. They could probably somehow get to my information on my phone. [After my negative experience with ICE,] I don't think we have privacy. I mean, I basically think they have access to anything they want. Because they did when they came to my house. They knew everything about us. Things that we were private about with others, they knew."*

With regard to membership in immigration-related groups, three participants expressed their uncertainty as they wondered out loud whether it put them at risk of being *"traced"* by ICE. However, this concern did not outweigh the benefit of those groups and participants continued to use them.

For the most part, the risks of surveillance were palpable, yet abstract. Participants could not pinpoint exact risks and instead feared that the government could see anything. Very few reported strategies they had developed to protect against surveillance. P2 described a strategy that her friend insisted they use when talking about political topics: placing their phones in the microwave. P12 avoided using certain words in messages and on social media, she and her friends used code words instead. However, while there is some concern that technology could amplify the risks of detection by authorities, there is a stronger sense of resignation that government authorities already have information about them, regardless of the technology choices they make.

Limited precautions

Finally, it is worth stressing that almost none of the participants in this study discussed using the privacy settings and controls available in the respective tools they actively use. While they have some strategies for seeking privacy and security as we discussed, they have a limited sense of risks and trade-offs, and

overall are not familiar with the range of choices they could employ to be safer online. We noted little interaction with fine-grained privacy controls, such as post-specific visibility settings or reviewing content visibility. Most participants knew about additional options to further customize privacy settings within Facebook, but did not use them.

DISCUSSION

Consistent with prior literature [45], our findings show that the undocumented immigrant community is indeed vulnerable in many ways, and our participants felt this vulnerability acutely. While some try to live their lives as "normally" as possible offline, others go to great lengths to mitigate risks. In their ICT use however, few of our participants worried nearly as much and do relatively little to address their vulnerability. While this behavior is consistent with general findings on privacy practices [50, 95], it is in glaring contrast to our population's level of vulnerability, the potential consequences of disclosure, and the extreme protective measures some of them take offline.

Factors Impeding Effective Privacy Protection

Why does a community with objectively higher risks do so little to protect themselves as they use technology in their daily lives? Madden [61] finds that Hispanic adults in the United States considered to have low socioeconomic status also have low technology literacy. However, our interviews suggest that low levels of digital literacy are not a sufficient explanation for our participants. There are at least four additional factors: (1) technology provides tremendous benefits to this community; (2) there is significant uncertainty about ICT-related risks specifically associated with their status; (3) they have high overall trust in the major social media platforms; and (4) a general belief that authorities are omniscient leads to a sense that any protective measures would be ineffective.

Benefits outweigh uncertain risks

Past research suggests that risk perception is based on two factors: how known the risk is, and the 'dread' factor of the risk [84]. If the risk is unknown, perceptions of its danger will decrease. Our participants did not see a direct line between technology-related actions and potential immigration-related consequences. There are few examples of technology leading to immigration enforcement, and there are no tangible clues in the digital environment that help users understand risks. This uncertainty likely contributes to a perception of low risk, which is in stark contrast to offline interactions, where risks are more tangible and better known. Most participants strove for a balance between unconstrained use of technology and complete abstention. For some, the benefits — communication, information and self-expression — outweighed uncertain risks. A small minority chose to abstain from engaging in social media and group communication.

Trust overrides critical risk assessment

Our participants place a relatively high degree of trust in their tools, likely bolstered by observations of peers actively using those tools and a sense of control over their data [18]. In addition, participants display trust toward the companies and platforms that mediate their online interactions. No one shared perceptions of harm or danger in relation to companies, even though these companies amass data for commercial interests and have to provide law enforcement access in certain circumstances. Scholz and Lubell [81] found that trust may serve as a heuristic that leads to the circumvention of effortful cognitive processing of potential risks. The trust our participants placed in service providers may lead them to bypass critical consideration of their role in disclosing sensitive information.

Resilience with resignation

Our participants took few privacy-enhancing actions in part because they felt that authorities have plenty of information about them. In this, they echo previous findings that if people already think their information is available elsewhere, they may be more reluctant to try to take precautions [4].

Similar behavior, amplified consequences

Most of our participants' security and privacy concerns were similar to those of the broader population, including concerns related to identity theft, monitoring children's online behavior, and unwanted contact by strangers. Studies among college students have found a broad range of strategies in managing self-disclosure and interpersonal disclosures [56, 97]. Our participants' privacy regulation strategies are similar, but different in two ways: First, they are limited to a few kinds of individually-focused, preventative behaviors primarily aimed to enable "intimate interaction" [97]. Second, the boundary turbulences they experience have amplified consequences.

Furthermore, while our participants have developed clear ideas about what physical spaces are relatively private or public, safe or less safe, these notions are eroding through the encroachment of technology. Social norms about how to protect others' privacy and security in shared communities are still underdeveloped. Everyone has a camera in their pocket, and the ability to instantly post photos with geolocation could jeopardize the safety of those depicted. Boundaries blur between online and offline privacy and security, which also affects boundaries they have expended much effort curating online.

Finally, the burden of self-censorship on a person's well-being can be oppressive [96, 97]. Extra stress could have negative implications for integration, further isolating undocumented persons and their families from the broader community.

Implications and Recommendations

Based on our findings, we have identified insights and recommendations for digital security education, community organization, and technology design, which may benefit not just undocumented immigrants but vulnerable communities in general.

Develop community-appropriate educational resources

Most of our participants felt their digital literacy was not as developed as they would like. We see an opportunity for educational resources about digital security developed for immigrant communities that incorporate their identities as individuals, parents, and undocumented immigrants. Indeed, almost all our participants were eager to improve their technology literacy and better protect themselves.

However, they do not seem to seek out available online resources, which means that compiling resources online — even

if optimized for mobile — is insufficient. Instead, knowledge could be brought into the community, preferably in the community's primary language; participants expressed strong interest in in-person trainings and workshops on technology use, privacy and security. Such efforts should be carefully discussed, coordinated and led by trusted community allies and support organizations. Done well, ICT educational efforts could contribute to the overall well-being and integration of undocumented and mix-status immigrant communities.

Take precaution with organizational communication practices
Allies should be aware of the risks of potentially revealing information about members in vulnerable communities. Organizations that hold information about their patrons and community members may inadvertently put undocumented immigrants at risk. Those that have a strong interest in protecting undocumented immigrants in their community, such as schools, churches, activist groups, and libraries, should evaluate their technology practices. For instance, special care should be taken when collecting or storing phone numbers given that their exposure could facilitate locating individuals.

Building new tools is not a priority
While designing new technology is a frequent impulse to help vulnerable communities, it is rarely successful [93]. From our interviews, it seems unlikely that our participants or their communities would adopt new tools or apps of their own volition. The fact that this community is largely not using fine-grained privacy settings further suggests that current privacy settings and tools might not be properly meeting users' needs. Furthermore, apps aimed at this community would stand out as observation targets for immigration enforcement. Instead, the focus should be on improving existing tools and on making privacy and security features more visible and usable.

Support on-demand information hiding
We find that this mobile-primary community carries and stores much of their digital information on their smartphones. If lost, searched or confiscated, smartphones may put the owner and others at risk. While many smartphones are already fully encrypted, the proliferation of usable authentication mechanisms, such as fingerprint or face recognition, may weaken practical security, as a person could be compelled to unlock a phone with biometric markers if detained [79]. More research should focus on means to enable information hiding on demand and plausible deniability on smartphones. An example in that direction is a feature in Apple's iOS 11: quickly pressing the home button five times temporarily deactivates fingerprint authentication and forces passcode entry [101].

Make information flows and audiences more transparent
The uncertainty about online risk of exposure contributes to concern and stress for most of our participants. The transparency of who has access to information and what entities participate in information flows requires further research attention. Prior research has shown that privacy nudges can increase awareness of a social media post's audience [99]. Research on increasing awareness and accurate understanding of information flows would benefit not only undocumented immigrants but also Internet users in general.

Limit exposure of identifying information
Service providers could reduce privacy concerns in group settings by limiting what group members can learn about each other. For instance, while messaging apps may rely on phone numbers as identifiers, phone numbers may not have to be visible to everyone in a shared group, making it more difficult to extract group members' contact information. Service providers and researchers should study and consider how desired affordances of social media platforms could be maintained while providing the opportunity for vulnerable communities to protect their identity on the platform.

Virtual sanctuary for undocumented immigrants
Companies, such as Facebook, should recognize that they are serving a variety of vulnerable communities, many of whom believe the platforms provide a safe space. They may want to embrace the role of guardian and protector of those communities. Platforms could strive to provide virtual sanctuary. This would mean re-examining what information their services collect, store, share, and expose to other users, in order to reduce opportunities to harm vulnerable communities with the data they have been entrusted with. These companies may also want to consider adopting stances akin to sanctuary cities in the United States. We hope large companies like Facebook, as transnational companies, would strive to protect all of their users, regardless of socio-political or physical borders.

CONCLUSION

For undocumented immigrants living in the United States, typical struggles of immigration and integration are exacerbated by a fear of discovery and deportation. How undocumented immigrants perceive and manage status-related risks in technology use has not been well understood previously. Through our interviews with 17 Latinx undocumented immigrants, we provide insights into this community's technology use practices, risk perceptions and protective strategies. We find that many struggle to translate awareness and risk mitigation strategies they employ in the physical world to technology use and the online environment. Due to uncertain risks of various kinds, including surveillance and a sense that the government knows a lot about them already, many do not fully consider how their behavior online may affect risks of discovery. For others, technology use is associated with tensions among convenience, intimate engagement, self-disclosure, self-censorship and community participation. Furthermore, we find latent yet uncertain concerns about what others in their network might inadvertently reveal about them. These tensions and boundary turbulences create stress that may affect the well-being of themselves and their families.

Our findings demonstrate an opportunity for the design and provision of educational resources, and the design of transparency and privacy mechanisms. Community organizations, such as schools or churches, as well as service providers, such as Facebook, also have an important role to play in mitigating, or potentially exacerbating, risks from technology use for the undocumented immigrant community and vulnerable communities more broadly.

ACKNOWLEDGMENTS

The authors thank all participants and the immigrant rights activists and community allies who supported this research. This research was funded by the University of Michigan School of Information.

REFERENCES

1. Ruba Abu-Salma, M Angela Sasse, Joseph Bonneau, Anastasia Danilova, Alena Naiakshina, and Matthew Smith. 2017. Obstacles to the Adoption of Secure Communication Tools. In *2017 IEEE Symposium on Security and Privacy (SP'17)*. IEEE Computer Society. DOI:http://dx.doi.org/10.1109/SP.2017.65
2. Alessandro Acquisti, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub, Manya Sleeper, Yang Wang, and Shomir Wilson. 2017. Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online. *ACM Comput. Surv.* 50, 3, Article 44 (Aug. 2017), 41 pages. DOI:http://dx.doi.org/10.1145/3054926
3. Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. 2015. Privacy and human behavior in the age of information. *Science* 347, 6221 (2015), 509–514. DOI:http://dx.doi.org/10.1126/science.aaa1465
4. Alessandro Acquisti, Leslie K John, and George Loewenstein. 2013. What is privacy worth? *The Journal of Legal Studies* 42, 2 (2013), 249–274.
5. Hazim Almuhimedi, Florian Schaub, Norman Sadeh, Idris Adjerid, Alessandro Acquisti, Joshua Gluck, Lorrie Faith Cranor, and Yuvraj Agarwal. 2015. Your Location Has Been Shared 5,398 Times!: A Field Study on Mobile App Privacy Nudging. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, New York, NY, USA, 787–796. DOI: http://dx.doi.org/10.1145/2702123.2702210
6. Tawfiq Ammari, Priya Kumar, Cliff Lampe, and Sarita Schoenebeck. 2015. Managing children's online identities: How parents decide what to disclose about their children online. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, 1895–1904. DOI: http://dx.doi.org/10.1145/2702123.2702325
7. Susan B. Barnes. 2006. A privacy paradox: Social networking in the United States. *First Monday* 11, 9 (2006). DOI:http://dx.doi.org/10.5210/fm.v11i9.1394
8. Luis Fernando Baron and Ricardo Gomez. 2017. *Living in the Limits: Migration and Information Practices of Undocumented Latino Migrants*. 147–158. DOI: http://dx.doi.org/10.1007/978-3-319-59111-7_13
9. Luis Fernando Baron, Moriah Neils, and Ricardo Gomez. 2014. Crossing new borders: computers, mobile phones, transportation, and English language among Hispanic day laborers in Seattle, Washington. *Journal of the Association for Information Science and Technology* 65, 1 (2014), 98–108. DOI:http://dx.doi.org/10.1002/asi.22949
10. Frank D Bean, Susan K Brown, and James D Bachmeier. 2015. *Parents without papers: The progress and pitfalls of Mexican American integration*. Russell Sage Foundation.
11. Alvaro M. Bedoya. 2017. Deportation is Going High-Tech Under Trump. *The Atlantic* (June 2017). https://www.theatlantic.com/technology/archive/2017/06/data-driven-deportation/531090/ [Online; Retrieved 17 September 2017].
12. Ali Behdad. 2005. *A Forgetful Nation: On Immigration and Cultural Identity in the United States*. Duke University Press.
13. Andrew Besmer and Heather Richter Lipford. 2010. Moving Beyond Untagging: Photo Privacy in a Tagged World. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '10)*. ACM, New York, NY, USA, 1563–1572. DOI: http://dx.doi.org/10.1145/1753326.1753560
14. Lindsay Blackwell, Jean Hardy, Tawfiq Ammari, Tiffany Veinot, Cliff Lampe, and Sarita Schoenebeck. 2016. LGBT Parents and Social Media: Advocacy, Privacy, and Disclosure During Shifting Social Movements. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. ACM, New York, NY, USA, 610–622. DOI: http://dx.doi.org/10.1145/2858036.2858342
15. Nikita Borisov, Ian Goldberg, and Eric Brewer. 2004. Off-the-record Communication, or, Why Not to Use PGP. In *Proceedings of the 2004 ACM Workshop on Privacy in the Electronic Society (WPES '04)*. ACM, New York, NY, USA, 77–84. DOI: http://dx.doi.org/10.1145/1029179.1029200
16. Christoph Bösch, Benjamin Erb, Frank Kargl, Henning Kopp, and Stefan Pfattheicher. 2016. Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns. *Proceedings on Privacy Enhancing Technologies* 2016, 4 (2016), 237–254. DOI: http://dx.doi.org/10.1515/popets-2016-0038
17. danah boyd. 2014. *It's Complicated: The Social Lives of Networked Teens*. Yale University Press.
18. Laura Brandimarte, Alessandro Acquisti, and George Loewenstein. 2013. Misplaced Confidences: Privacy and the Control Paradox. *Social Psychological and Personality Science* 4, 3 (2013), 340–347. DOI: http://dx.doi.org/10.1177/1948550612455931
19. Russell Brandom. 2017. The US Border Patrol is trying to build face-reading drones. (6 April 2017). https://www.theverge.com/2017/4/6/15208820/customs-border-patrol-drone-facial-recognition-silicon-valley-dhs [Online; Retrieved 17 September 2017].

20. Susan K. Brown and Alejandra Jazmin Sanchez. 2017. Parental Legal Status and the Political Engagement of Second-Generation Mexican Americans. *RSF: The Russell Sage Foundation Journal of the Social Sciences* 3, 4 (2017), 136–47. DOI: http://dx.doi.org/10.7758/RSF.2017.3.4.08

21. Andreas Buchenscheit, Bastian Könings, Andreas Neubert, Florian Schaub, Matthias Schneider, and Frank Kargl. 2014. Privacy Implications of Presence Sharing in Mobile Messaging Applications. In *Proceedings of the 13th International Conference on Mobile and Ubiquitous Multimedia (MUM '14)*. ACM, New York, NY, USA, 20–29. DOI:http://dx.doi.org/10.1145/2677972.2677980

22. Jenna Burrell and Ken Anderson. 2008. 'I have great desires to look beyond my world': trajectories of information and communication technology use among Ghanaians living abroad. *New Media & Society* 10, 2 (2008), 203–224. DOI: http://dx.doi.org/10.1177/1461444807086472

23. Ricardo Castro-Salazar and Carl Bagley. 2010. 'Ni de aqui ni from there': Navigating Between Contexts: Counter-Narratives of Undocumented Mexican Students in the United States. *Race Ethnicity and Education* 13, 1 (2010), 23–40. DOI: http://dx.doi.org/10.1080/13613320903549651

24. Daphne Chang, Erin L. Krupka, Eytan Adar, and Alessandro Acquisti. 2016. Engineering Information Disclosure: Norm Shaping Designs. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. ACM, New York, NY, USA, 587–597. DOI:http://dx.doi.org/10.1145/2858036.2858346

25. Leo R. Chavez. 2012. *Shadowed Lives: Undocumented Immigrants in American Society* (third ed.). Wadsworth.

26. Jay Chen, Michael Paik, and Kelly McCabe. 2014. Exploring Internet Security Perceptions and Practices in Urban Ghana. *In Proc. Symposium on Usable Privacy and Security (SOUPS '14)* 14 (2014). https://www.usenix.org/conference/soups2014/proceedings/presentation/chen

27. Wenli Chen. 2010. Internet-usage patterns of immigrants in the process of intercultural adaptation. *Cyberpsychology, Behavior, and Social Networking* 13, 4 (2010), 387–399. DOI: http://dx.doi.org/10.1089/cyber.2009.0249

28. Wenli Chen and Wenting Xie. 2012. *Cyber behaviors of immigrants*. Encyclopedia of Cyber Behavior, 259-272.

29. Mathew Coleman. 2012. The "Local" Migration State: The Site-Specific Devolution of Immigration Enforcement in the U.S. South. *Law & Policy* 34, 2 (2012), 159–190. DOI: http://dx.doi.org/10.1111/j.1467-9930.2011.00358.x

30. Sasha Constanza-Chock. 2011. Digital Popular Communication Lessons on Information and Communication Technologies for Social Change from the Immigrant Rights Movement National. *Civic Review* (Fall 2011), 29–35. DOI:http://dx.doi.org/10.1002/ncr.20065

31. Stephen M. Croucher. 2011. Social networking and cultural adaptation: A theoretical model. *Journal of International and Intercultural Communication* 4, 4 (2011), 259–264. DOI: http://dx.doi.org/10.1080/17513057.2011.598046

32. Ralf De Wolf, Koen Willaert, and Jo Pierson. 2014. Managing privacy boundaries together: Exploring individual and group privacy management strategies in Facebook. *Computers in Human Behavior* 35 (2014), 444–454. DOI:http://dx.doi.org/10.1016/j.chb.2014.03.010

33. Department of Homeland Security. 2012. Exercising Prosecutorial Discretion wiht Respect to Individuals Who Came to the United States as Children. (15 June 2012). https://www.dhs.gov/xlibrary/assets/s1-exercising-prosecutorial-discretion-individuals-who-came-to-us-as-children.pdf [Online; Retrieved 17 September 2017].

34. Diaspora. 2017. (2017). https://diasporafoundation.org/.

35. Roger Dingledine, Nick Mathewson, and Paul Syverson. 2004. Tor: The second-generation onion router. Usenix. http://static.usenix.org/legacy/events/sec04/tech/dingledine.html

36. Nicole B. Ellison, Charles Steinfield, and Cliff Lampe. 2011. Connection strategies: Social capital implications of Facebook-enabled communication practices. *New Media & Society* 13, 6 (2011), 873–892. DOI: http://dx.doi.org/10.1177/1461444810385389

37. Laura E. Enriquez. 2011. 'Because We Feel the Pressure and We Also Feel the Support': Examining the Educational Success of Undocumented Immigrant Latina/o Students. *Harvard Educational Review* 81, 3 (2011), 476–500. DOI: http://dx.doi.org/10.17763/haer.81.3.w7k703q050143762

38. Adolfo Flores. 2017. People Are Worried About DHS Plans To Gather Social Media Info. *Buzzfeed News* (September 2017). https://www.buzzfeed.com/adolfoflores/people-are-worried-about-dhs-plans-to-gather-social-media [Online; Retrieved 17 September 2017].

39. Welcoming Center for New Pennsylvanians. 2012. *Digital Diaspora: How Immigrants Are Capitalizing on Today's Technology*. Philadelphia. http://www.welcomingcenter.org/sites/default/files/digital_diaspora_final_report_-_nov_2012.pdf

40. Forbes On Marketing. 2012. Social Media And The Big Data Explosion. (Jul 2012). https://www.forbes.com/sites/onmarketing/2012/06/28/social-media-and-the-bigdata-explosion/#58a8c1766a61

41. Simson Garfinkel and Heather Richter Lipford. 2014. Usable Security: History, Themes, and Challenges. *Synthesis Lectures on Information Security, Privacy, and Trust* 5, 2 (2014), 1–124. DOI: http://dx.doi.org/10.2200/S00594ED1V01Y201408SPT011

42. Ruth Gomberg-Muñoz. 2011. *Labor and Legality: An Ethnography of a Mexican Immigrant Network*. Oxford University Press, New York.

43. Ricardo Gomez and Sara Vannini. 2015. *Fotohistorias: Participatory Photography and the Experience of Migration*. CreateSpace Independent Publishing Platform, Seattle, WA.

44. Roberto G. Gonzales and Leo R. Chavez. 2012. "Awakening to a Nightmare": Abjectivity and Illegality in the Lives of Undocumented 1.5-Generation Latino Immigrants in the United States. *Current Anthropology* 53, 3 (2012), 255–281. DOI: http://dx.doi.org/10.1086/665414

45. Roberto. G. Gonzales and Steven Raphael. 2017. Illegality: A Contemporary Portrait of Immigration. *RSF: The Russell Sage Foundation Journal of the Social Sciences* 3, 4 (2017), 1–17. https://dx.doi.org/10.7758/RSF.2017.3.4.01

46. Glen Greenwald. 2014. *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. Metropolitan Books.

47. Ralph Gross and Alessandro Acquisti. 2005. Information Revelation and Privacy in Online Social Networks. (2005), 71–80. DOI: http://dx.doi.org/10.1145/1102199.1102214

48. Lauren E. Gulbas and Luis H. Zayas. 2017. Exploring the Effects of U.S Immigration Enforcement on the Well-being of Citizen Children in Mexican Immigrant Families. *RSF: The Russell Sage Foundation Journal of the Social Sciences* 3, 4 (2017), 53–69. https://doi.org/10.7758/RSF.2017.3.4.04

49. Lisa J Hardy, Christina M Getrich, Julio C Quezada, Amanda Guay, Raymond J Michalowski, and Eric Henley. 2012. A call for further research on the impact of state-level immigration policies on public health. *American journal of public health* 102, 7 (2012), 1250–1253.

50. Eszter Hargittai and Alice Marwick. 2016. "What Can I Really Do?" Explaining the Privacy Paradox with Online Apathy. *International Journal of Communication* 10 (2016), 3737–3757. http://ijoc.org/index.php/ijoc/article/view/4655

51. Bernie Hogan. 2010. The Presentation of Self in the Age of Social Media: Distinguishing Performances and Exhibitions Online. *Bulletin of Science, Technology & Society* 30, 6 (2010), 377–386. DOI: http://dx.doi.org/10.1177/0270467610385893

52. Iulia Ion, Rob Reeder, and Sunny Consolvo. 2015. "...no one can hack my mind": Comparing Expert and Non-Expert Security Practices. *In Proc. Symposium on Usable Privacy and Security (SOUPS'15), USENIX* (2015). https://www.usenix.org/system/files/conference/soups2015/soups15-paper-ion.pdf

53. Michael Jones-Correa and James A. McCann. 2016. In the Public but Not the Electorate: The "Civic Status Gap" in the United States. *RSF: The Russell Sage Foundation Journal of the Social Sciences* 2, 3 (2016), 1–19. https://doi.org/10.7758/rsf.2016.2.3.01

54. Anil Kalhan. 2013. Immigration Policing and Federalism Through the Lens of Technology, Surveillance and Privacy. *Ohio State Law Journal* 74 (2013). https://ssrn.com/abstract=2316327

55. Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. 2015. "My Data Just Goes Everywhere:" User Mental Models of the Internet and Implications for Privacy and Security. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. USENIX Association, Ottawa, 39–52. https://www.usenix.org/conference/soups2015/proceedings/presentation/kang

56. Airi Lampinen, Vilma Lehtinen, Asko Lehmuskallio, and Sakari Tamminen. 2011. We're in it together: Interpersonal Management of Disclosure in Social Network Services. *In Proc. SIGCHI Conference on Human Factors in Computing Systems (CHI '11) ACM* (2011), 3217–3226.

57. Jialiu Lin, Shahriyar Amini, Jason I. Hong, Norman Sadeh, Janne Lindqvist, and Joy Zhang. 2012. Expectation and Purpose: Understanding Users' Mental Models of Mobile App Privacy Through Crowdsourcing. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing (UbiComp '12)*. ACM, New York, NY, USA, 501–510. DOI: http://dx.doi.org/10.1145/2370216.2370290

58. Dara Lind. 2017. Fewer immigrants are being deported under Trump than under Obama: But it's not because Trump isn't trying. *Vox* (Aug. 2017). https://www.vox.com/policy-and-politics/2017/8/10/16119910/trump-deportations-obama [Online; Retrieved 17 September 2017].

59. Eden Litt and Eszter Hargittai. 2014. A bumpy ride on the information superhighway: Exploring turbulence online. *Computers in Human Behavior* 36 (2014), 520–529. https://doi.org/10.1016/j.chb.2014.04.027

60. William D Lopez, Daniel J Kruger, Jorge Delva, Mikel Llanes, Charo Ledón, Adreanne Waller, Melanie Harner, Ramiro Martinez, Laura Sanders, Margaret Harner, and others. 2017. Health Implications of an immigration raid: findings from a Latino community in the Midwestern United States. *Journal of immigrant and minority health* 19, 3 (2017), 702–708.

61. Mary Madden. 2017. *Privacy, Security, and Digital Inequality*. Research report. Data & Society. https://datasociety.net/output/privacy-security-and-digital-inequality/

62. Mastodon. 2017. Decentralized Social Network. (2017). https://mastodon.social.

63. Tara Matthews, Kathleen O'Leary, Anna Turner, Manya Sleeper, Jill Palzkill Woelfer, Martin Shelton, Cori Manthorne, Elizabeth F. Churchill, and Sunny Consolvo. 2017. Stories from Survivors: Privacy & Security Practices when Coping with Intimate Partner Abuse. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. ACM, New York, NY, USA, 2189–2201. DOI: http://dx.doi.org/10.1145/3025453.3025875

64. Roger C Mayer, James H Davis, and F David Schoorman. 1995. An integrative model of organizational trust. *Academy of management review* 20, 3 (1995), 709–734.

65. Susan McGregor, Franziska Roesner, and Kelly Caine. 2016. Individual versus Organizational Computer Security and Privacy Concerns in Journalism. *Proc. Privacy Enhancing Technologies* 4 (2016). https://doi.org/10.1515/popets-2016-0048

66. Cecilia Menjívar. 2006. Liminal Legality: Salvadoran and Guatemalan Immigrants' Lives in the United States. *Amer. J. Sociology* 111, 4 (2006), 999–1037. https://doi.org/10.1086/499509

67. Brian Naylor. 2017. Trump's Plan To Hire 15,000 Border Patrol And ICE Agents Won't Be Easy. (February 2017). http://www.npr.org/2017/02/23/516712980/trumps-plan-to-hire-15-000-border-patrol-and-ice-agents-wont-be-easy-to-fulfill [Online; Retrieved 17 September 2017].

68. Helen Nissenbaum. 2009. *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

69. Patricia A. Norberg, Daniel R. Horne, and David A. Horne. 2007. The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *J Consumer Affairs* 41, 1 (2007), 100–126. DOI: http://dx.doi.org/10.1111/j.1745-6606.2006.00070.x

70. Nicole Novak, Arline T. Geronimus, and Aresha M. Martinez-Cardoso. 2017. Change in birth outcomes among infants born to Latina mothers after a major immigration raid. *International Journal of Epidemiology* 46, 3 (1 June 2017), 839–849. https://doi.org/10.1093/ije/dyw346

71. Michael A. Olivas. 2007. Immigration-Related State and Local Ordinances: Preemption, Prejudice, and the Proper Role for Enforcement. *University of Chicago Legal Forum* 2007, 1 (2007). https://ssrn.com/abstract=1069121

72. Jeffrey S. Passel and D'Vera Cohn. 2017. As Mexican share declined, U.S. unauthorized immigrant population fell in 2015 below recession level. Fact Tank, Pew Research Center. (2017). http://www.pewresearch.org/fact-tank/2017/04/25/as-mexican-share-declined-u-s-unauthorized-immigrant-population-fell-in-2015-below-recession-level/ [Online; Retrieved 17 September 2017].

73. Sandra Petronio. 2010. Communication Privacy Management Theory: What Do We Know About Family Privacy Regulation? *Journal of Family Theory & Review* 2, 3 (2010), 175–196. DOI: http://dx.doi.org/10.1111/j.1756-2589.2010.00052.x

74. C. Phelan, C. Lampe, and P. Resnick. 2016. It's Creepy But It Doesn't Bother Me. CHI. https://doi.org/10.1145/2858036.2858381

75. Alejandro Portes and Rubén G. Rumbaut. 2006. *Immigrant America: A Portrait*. Univ. of California Press.

76. Emilee Rader, Rick Wash, and Brandon Brooks. 2012. Stories as informal lessons about security. *In Proceedings of the Eighth Symposium on Usable Privacy and Security (SOUPS '12). ACM* 6 (2012), 17. https://doi.org/10.1145/2335356.2335364

77. Ashwini Rao, Florian Schaub, Norman Sadeh, Alessandro Acquisti, and Ruogu Kang. 2016. Expecting the unexpected: Understanding mismatched privacy expectations online. *In Proc. Symposium on Usable Privacy and Security (SOUPS '16)* (2016). https://www.usenix.org/conference/soups2016/technical-sessions/presentation/rao

78. Rubén G. Rumbaut and Alejandro Portes. 2001. *Ethnicities: Children of immigrants in America*. Univ. of California Press.

79. Erin M Sales. 2014. The Biometric Revolution: An Erosion of the Fifth Amendment Privilege to Be Free from Self-Incrimination. *U. Miami L. Rev.* 69 (2014), 193. https://ssrn.com/abstract=2410688

80. Bruce Schneier. 2015. *Data and Goliath: The hidden battles to collect your data and control your world*. WW Norton & Company.

81. John T Scholz and Mark Lubell. 1998. Trust and taxpaying: Testing the heuristic approach to collective action. *American Journal of Political Science* (1998), 398–417.

82. Fatemeh Shirazi and Melanie Volkamer. 2014. What Deters Jane from Preventing Identification and Tracking on the Web?. In *Proceedings of the 13th Workshop on Privacy in the Electronic Society (WPES '14)*. ACM, New York, NY, USA, 107–116. DOI: http://dx.doi.org/10.1145/2665943.2665963

83. Dawinder Sidhu. 2007. The Chilling Effect of Government Surveillance Programs on the Use of the Internet By Muslim-Americans (June 27, 2011). *University of Maryland Law Journal of Race, Religion, Gender and Class* 7 (2007), 375. https://ssrn.com/abstract=1002145

84. Paul Slovic. 1987. Perception of risk. *Science* 236, 4799 (1987), 280–285.

85. Robert Snell. 2017. Feds use anti-terror tool to hunt the undocumented. (18 May 2017). http://www.detroitnews.com/story/news/local/detroit-city/2017/05/18/cell-snooping-fbi-immigrant/101859616/ [Online; Retrieved 17 September 2017].

86. Carola Suárez-Orozco, Marcelo M. Suárez-Orozco, and Irina Todorova. 2009. *Learning a New Land: Immigrant Students in American Society*. Harvard University Press.

87. Linnet Taylor, Luciano Floridi, and Bart van der Sloot (Eds.). 2017. *Group Privacy*. Springer International Publishing. DOI: http://dx.doi.org/10.1007/978-3-319-46608-8

88. Paul Taylor, Mark H. Lopez, Jeffrey S. Passel, and Seth Motel. 2011. Unauthorized Immigrants: Length of Residency, Patterns of Parenthood. Pew Hispanic Center. (2011). http://assets.pewresearch.org/wp-content/uploads/sites/7/2011/12/Unauthorized-Characteristics.pdf

89. The American Civil Liberties Union of Vermont. 2017. ACLU Demands Immediate End to DMV Facial Recognition Program. Press Release. (24 May 2017). https://www.acluvt.org/en/press-releases/aclu-demands-immediate-end-dmv-facial-recognition-program [Online; Retrieved 17 September 2017].

90. The White House. 2017a. Executive Order 13767. (25 January 2017). https://www.whitehouse.gov/the-press-office/2017/01/25/executive-order-border-security-and-immigration-enforcement-improvements [Online; Retrieved 17 September 2017].

91. The White House. 2017b. Executive Order 13768. (25 January 2017). https://www.whitehouse.gov/the-press-office/2017/01/25/presidential-executive-order-enhancing-public-safety-interior-united [Online; Retrieved 17 September 2017].

92. The White House. 2017c. Executive Order 13769. (25 January 2017). https://www.whitehouse.gov/the-press-office/2017/01/27/executive-order-protecting-nation-foreign-terrorist-entry-united-states [Online; Retrieved 17 September 2017].

93. Kentaro Toyama. 2015. *Geek Heresy: Rescuing Social Change from the Cult of Technology*. PublicAffairs.

94. Jenny Hsin-Chun Tsai. 2006. Use of Computer Technology to Enhance Immigrant Families' Adaptation. *Journal of Nursing Scholarship* 38, 1 (2006), 87–93. DOI: http://dx.doi.org/10.1111/j.1547-5069.2006.00082.x

95. Joseph Turow, Michael Hennessy, and Nora Draper. 2015. *The Tradeoff Fallacy: How Marketers are Misrepresenting American Consumers and Opening Them up to Exploitation. Report*. Annenberg School of Communication, University of Pennsylvania. https://www.asc.upenn.edu/news-events/publications/tradeoff-fallacy-how-marketers-are-misrepresenting-american-consumers-and

96. Jessica Vitak. 2012. The Impact of Context Collapse and Privacy on Social Network Site Disclosures. *Journal of Broadcasting & Electronic Media* 56, 4 (2012), 451–470. DOI:http://dx.doi.org/10.1080/08838151.2012.732140

97. Jessica Vitak and Jinyoung Kim. 2014. "You Can't Block People Offline": Examining How Facebook's Affordances Shape the Disclosure Process. In *Proceedings of the 17th ACM Conference on Computer Supported Cooperative Work & Social Computing (CSCW '14)*. ACM, New York, NY, USA, 461–474. DOI: http://dx.doi.org/10.1145/2531602.2531672

98. Kaveh Waddell. 2017. 'Give Us Your Passwords'. *The Atlantic* (February 2017). https://www.theatlantic.com/technology/archive/2017/02/give-us-your-passwords/516315/ [Online; Retrieved 17 September 2017].

99. Yang Wang, Pedro Giovanni Leon, Alessandro Acquisti, Lorrie Faith Cranor, Alain Forget, and Norman Sadeh. 2014. A Field Trial of Privacy Nudges for Facebook. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '14)*. ACM, New York, NY, USA, 2367–2376. DOI: http://dx.doi.org/10.1145/2556288.2557413

100. Yang Wang, Gregory Norcie, Saranga Komanduri, Alessandro Acquisti, Pedro Giovanni Leon, and Lorrie Faith Cranor. 2011. "I Regretted the Minute I Pressed Share": A Qualitative Study of Regrets on Facebook. In *Proceedings of the Seventh Symposium on Usable Privacy and Security (SOUPS '11)*. ACM, New York, NY, USA, Article 10, 16 pages. DOI: http://dx.doi.org/10.1145/2078827.2078841

101. Tom Warren. 2017. iOS 11 has a 'cop button' to temporarily disable Touch ID. The Verge, Aug. 17, 2017. (2017). https://www.theverge.com/2017/8/17/16161758/ios-11-touch-id-disable-emergency-services-lock accessed: Sept. 17, 2017.

102. Alma Whitten and J. D. Tygar. 1999. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In *Proceedings of the 8th Conference on USENIX Security Symposium*. USENIX Association. http://dl.acm.org/citation.cfm?id=1251421.1251435

103. Jill Palzkill Woelfer and David G Hendry. 2010. Homeless young people's experiences with information systems: life and work in a community technology center. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 1291–1300.

104. Svetlana Yarosh. 2013. Shifting dynamics or breaking sacred traditions? the role of technology in twelve-step fellowships.. In *Proc. Conference on Human Factors in Computing (CHI '13)*. ACM.

105. Hirokazu Yoshikawa. 2011. *Immigrants Raising Citizens: Undocumented Parents and Their Children*. Russell Sage Foundation.

106. Reza Zafarani, Mohammad Ali Abbasi, and Huan Liu. 2014. *Social media mining: an introduction*. Cambridge University Press.

107. Philip R. Zimmermann. 1995. *The Official PGP User's Guide*. MIT Press, Cambridge, MA, USA.