Straight Talk

NEW YORKERS ON MOBILE MESSAGING AND IMPLICATIONS FOR PRIVACY

https://simplysecure.org/resources/techreports/NYC15-MobMsg.pdf

Ame Elliott, Design Director
ame@simplysecure.org

Sara Brody, Executive Director
scout@simplysecure.org

Simply Secure

Preliminary draft; please send questions & feedback

Table of Contents

Introduction

In December 2015, Simply Secure conducted field research in New York City with 12 low-income African-Americans from Harlem and Brownsville. Our goal was to understand attitudes about mobile messaging and identify design directions for privacy-preserving software. Through in-context, semi-structured interviews we discussed participants' 1) current messaging practices, 2) motivations for using their preferred messaging apps, and 3) thoughts on privacy and surveillance (both physical and digital).

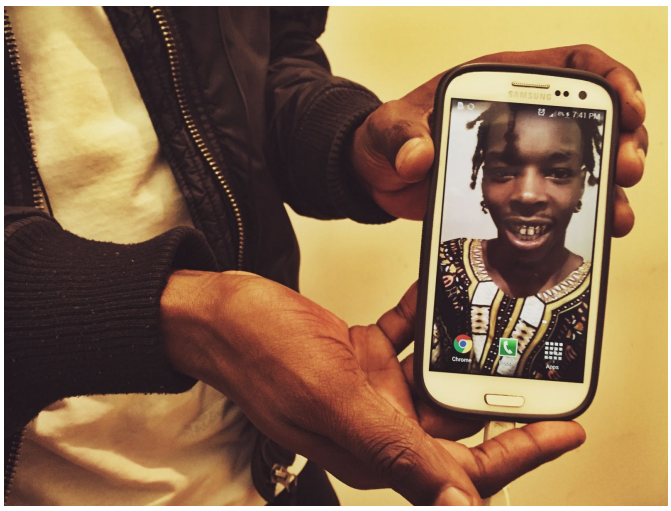
Our findings indicate a significant gap between the priorities of the low-income African-Americans in our study and much of the security and privacy community, both academic and industrial. This report shares how social, economic, and technical systems shape priorities for secure communication among our participants. Against a backdrop of inevitable surveillance, participants shared their:

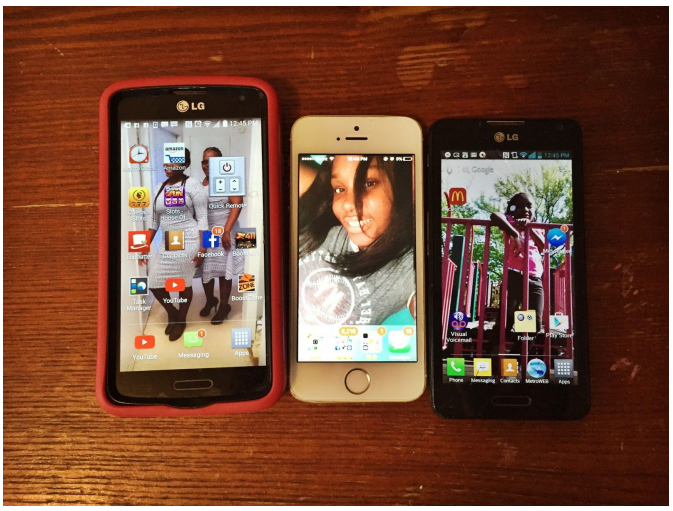
1. concerns about physical device security, particularly shoulder surfing
2. negative consequences of family-plan group billing arrangements giving unwanted access
3. renter's mindset that the handset is controlled by an adversarial carrier.

We share more details on the study design throughout the document in sidebars. After presenting our research findings, we conclude with design directions for practitioners seeking to build privacy-preserving software with broad appeal.

Motivation

We set out to get insight into the privacy needs of low-income people of color in urban areas of the United States. There is a long history of surveillance of African-Americans dating back to the earliest days of the country [1], while recent reports show people of color being disproportionately targeted by surveillance from law enforcement [2]. While other efforts in the internet-freedom space have explored the needs of populations at risk around the globe (e.g. Tibetan Activists [3]), there has been comparatively little attention paid to the domestic context. Moreover, people of color are underrepresented in many current conversations around data privacy, encryption, and government surveillance [4].





We were interested in comparing participants' responses to those of a larger-sample benchmark, such as the Pew Internet Study of Americans' attitudes to privacy and surveillance [5]. Additionally, part of Simply Secure's mission is to make privacy-preserving tools accessible to a broad audience, so we wanted to learn more about participants' needs to help for advocate them among software developers.

Mobile messaging is interesting because smart phones have come to be an essential communication technology both in the US and internationally, and the next billion online will be mobile-first and will not consider the desktop experience the default. In the United States, 68% of adults own smartphones, and ownerships cuts across races and incomes [5].

Surveillance is inevitable, and privacy is impossible

In recruiting participants we sought people who have a smartphone and are a regular user of at least one messaging app. We did not screen based on their attitudes towards surveillance, knowledge of security, or concerns about privacy. Although Brownsville and Harlem have robust activist communities with technical security skills in circumventing surveillance, these participants did not self-identify as concerned about surveillance.

Participants told us about how the social, economic, and technical systems surrounding them shape their priorities for secure communication. Time and again, participants expressed that they find no safe harbor from surveillance at home, at work, or in public. Participants' lived experience of surveillance spanned:

- Physical environments
- Social relationships
- Cellphone carriers
- Device hardware
- Application use

The overarching message we took from this study is that if you're poor and Black, surveillance in your daily life is the norm. Everything you do is suspect, and you're always on camera, and always at risk of being accused of some crime. Many of the participants work in retail and are on camera the entire time they are on the job, presumably as a deterrent against theft. If you work at Chipotle, or Best Buy, or Foot Locker, as some of our participants did, you are assumed to be stealing, and constantly under a supposition of guilt. Appealing to the video was viewed as a possible tool for proving innocence.

Physical Environments: Surveillance at Work, Home, and On the Go

Workplace policies also impact participants' mobile messaging use, as retail stores may prohibit employees from carrying a phone while on the clock or on the sales floor. Employees are assumed to be unprofessional or distractible, so many employers ban participants from having personal phones on their person while working. Upscale establishments have private lockers to store possessions while on the floor, but even in cases where lockers are provided, they are not always secure. One participant reported that employees of a neighborhood

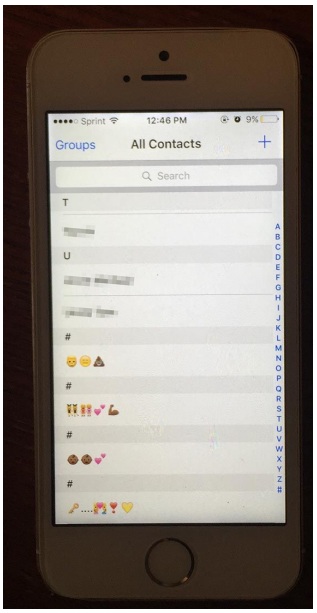
Participant Recruitment

Participants were recruited through Blue Ridges Labs, a social incubator focused on economic inclusion in New York. Blue Ridge Labs connected us with African-American participants from Harlem and Brownsville (their program's focus areas) who had smart phones and used at least one messaging app. They were not screened on the basis of attitudes towards surveillance, knowledge of security, or concerns about privacy.

Everyone was an adult with a mobile phone (10 Android, 2 iPhone), and was an enthusiastic user of messaging apps, sending at least 30 a week and some sending more than 100. Participants were not screened on the basis of privacy attitudes. Accompanied by a guide familiar with the participants and their communities, we gained intimate access to places and stories different than the academic and corporate campuses where security research traditionally takes place.

sneaker store may be forced to give their manager their phones when they start their shifts.

The experience of surveillance extends beyond the workplace and into to public spaces, which are often filled with video cameras or potentially-suspicious people, and to the home. Participants stated that economics keep people in their lives in unsafe living situations, sharing housing with people they don't trust. Physical threats to information security, including shoulder surfing and someone going through their phone, were a common theme. Social dynamics may make it awkward to take your phone with you when you leave a room to go to the bathroom , and using a screen lock (or failing to share the unlock code) can be interpreted as perceiving those around you as untrustworthy.



One ingenious solution that one 18 year old woman shared was to use emoji instead of names in a contact list. This makes snooping at a glance more difficult. Even though it's easy to reverse engineer who a contact is with sustained access, this approach has two benefits: 1) resilience to shoulder surfing, 2) plausible deniability for screen-shotting.

Participants mentioned SnapChat as being generous and protective of users by alerting them to when their chats had been captured by their correspondent via screenshot. Even though there are other mechanisms for capturing on-screen content, SnapChat's notification is seen as a good-faith indicator that SnapChat has their users' backs. In a world where the phone company owns the device and has ultimate access to its content, the security provided by SnapChat's model of auto-deleting messages is seen as distinctly positive.

Social Relationships: Family Plans and Surveillance

Surveillance by friends and family, such as parents surveilling children or partners surveilling each other, was very common. Some participants viewed iPhone's FaceTime unfavorably since it removed the ability to lie about your location via text. If you are known to have an iPhone, people (family members, or – in the case of one participant – an employer) can ask you to FaceTime to prove you are where you say you are. Counterintuitively, participants saw the reliability of the iPhone's camera as undesirable. If you tell people that your Android camera is broken, people accept it without

Research Methods

Activities:
1) in-context, semi-structured interviews in homes, restaurants, and libraries with dyads of mothers and daughters or cousins (90 min.)

2) a group interview of four young men at the office of a non-profit social entrepreneurship incubator in Brooklyn (60 min).

Semi-Structured Interview Guide:
- Ice-breaker, rapport builder
- Current messaging practices, apps used, & why
- Thoughts on privacy
- Feedback on app-store descriptions of secure messaging app

question, but the reliability of the iPhone subjects people to more culturally-enforced surveillance by people in their life.

In the Apple ecosystem, Family Sharing is positioned as making it easier to share content, but it can also provide opportunities for surveillance. In addition to manual location verification through FaceTime, the platform allows family members opted in to Family Sharing to see one another's live location directly on a map. This can pose a real risk to participants' safety and well-being. Similarly, one young man was glad to be rid of his iPhone because his estranged ex had tracked his movements with the Find My iPhone app, presumably because the ex had his iCloud password.

> *People remained trapped in plans with estranged partners, distant family members, and others they didn't know well.*

Just as economics can drive people into unsafe living conditions with people they don't trust, the cost of cellular service drives people into family plans with people with whom they have an adversarial relationship. Saving money with a group plan is a powerful incentive. Combined with inertia and an aggressive customer retention industry, our participants were in legacy family plans that no longer reflected their family or living situation. People remained trapped in plans with estranged partners, distant family members, and others they didn't know well, such as temporary roommates, or people they'd lost touch with.

One young man shared how his former partner impersonated him to the phone company and got printouts of all his text messages. His partner knew his birthdate and addresses, and either guessed codes or socially-engineered her way past account safeguards. Two participants shared that estranged ex-partners in their family plan had turned off their phone service just to mess with them. Their malice or need to control had dire economic consequences for the participants, as without phone number continuity their employment was disrupted.

Cell Phone Carriers: The Renters' Mindset

Many participants were part of the gig economy, which economists define as working for temporary help agencies, as independent contractors, or on-call. This type of work is a growing sector of the American economy, comprising 15.8% of American workers in the fall of 2015, up from 10.1 percent a decade earlier [7].

Participants with regular jobs but irregular hours are expressly vulnerable to phone-service disruption. Shift work and on-call labor means that people need to wait to be contacted by phone to come into work, and then expect to be sent home if it gets slow.

> *They consider themselves to be renting the hardware from the provider, who ultimately owns both the device and the data contained therein.*

A working phone is not only a vital economic lifeline, but also important tool for personal safety, well-being and support through communicating with others. Most participants use low-cost phones that come for free as part of a cellular service contract and upgrade their hardware infrequently. The participants had strongly adversarial relationships with the cell phone providers, like Cricket or Metro PCS, that they saw as a threat to the reliability of their phones. In particular, they believed the carriers were trying to push software updates to their phones to break them, which would in turn would force them to upgrade. This would represent a financial benefit the carrier, at the expense of the participant's job, safety, and well-being.

This adversarial relationship with carriers parallels an adversarial relationship with a landlord, so we term this view "renters' mindset." Participants know the providers own the device and that their monthly payment is a small portion, or rental-sized amount, of the total device value. They thus consider themselves to be renting the hardware from the provider, who ultimately owns both the device and the content contained therein. In the participants' world, there's no way to hide activities on the phone from the carrier landlord.

Consent and Ethics

Our partner, Blue Ridge Labs, handled the recruiting and led us to meet participants. We did not know their addresses, names, or contact information, an important step to protecting their privacy. As part of our consent process, participants understood that they could give us an assumed name, disappear back into New York, and we would have no way to find them.

Participants were also given a Participants' Bill of Rights (see the Resources section for a link to download) outlining consent procedures, including ability to refuse any questions or quit and still be compensated.

During our interviews, we showed participants images from the Humans of New York (HONY) Instagram feed [6] – which they were all familiar with – as an example how we might share their stories and personally-identifiable photos on the public web.

Participants then had the option of 3 levels of photographic participation.

- No photography
- Photographed in non-identifiable ways (such as their shoes or purses),
- Photographed in an identifiable way and signed a model release allowing their images to be shared publicly.

This extra step is important for Simply Secure, as we strive to strike a balance between sharing photos and stories to build empathy and protecting participants' privacy.

Hardware: Storage Space, Glitches, and Crashes

Because a working phone is so crucial in participants' personal and professional lives, their caution around software that might compromise its reliability extends beyond system updates. Storage space on the phone is at a premium. Most participants had older Android handsets pre-installed with what technologists would call "bloatware" – software provided by the carrier and that users see as useless to them, but which suffers from poor performance and cannot be uninstalled. Storage space is limited to the point that participants report having to delete an old app to make room for new ones. This means that any new app, such as a new secure-messaging alternative, must earn its way onto the device.

The original study plan included an option for participants to either use an Android phone with messaging software installed or to install a new app on their phones. We planned to have them give feedback on the app's interface by completing tasks with the interviewer. In the end, we decided against including messaging tasks, in part because asking participants to delete something else to make space for a new app would impose an undue burden.

In addition to storage-related concerns, people were very conservative about anything that made their phone "glitch," their preferred term for describing any software crash or malfunction. In contrast to the open-source ethos of embracing buggy software to support and improve it, the participants were much more protective of their computing environments Several cited a "one-strike policy": if an app glitched or made their phone crash, that's it, it's deleted. This points out a high barrier to entry for experimental open-source software, and points to a structural barrier that would limit these participants' engagement with the open source community more broadly.

In-App Surveillance: Feds in Facebook

In addition to the belief that cellular carriers can oversee what happens on the phone, as a landlord might have keys to a rental apartment, the participants shared a conviction that governments monitor online behavior. Three of the participants discussed specifically how the U.S. Government monitors communications, with one

sharing her belief that the NSA monitors Facebook accounts and kicks down the doors of people posting "risky" things. Another participant shared his experience of being racially profiled and pulled out of his car in Brownsville; in the same breath he spoke of how the "Feds read all the messages to see if something is up." He seemed resigned to this reality and had a detailed explanation for the necessity of government monitoring of messages. Similarly, one woman shared her unwillingness to speak on the phone in Spanish about someone's undocumented immigration status because she believes all calls are monitored and could result in someone being deported if they mentioned being undocumented on a call.

The most striking example of government monitoring was during the focus group of young men, who shared stories of how police "catfish" people in the community on Facebook. "Catfishing" was a widely-used phrase among participants, one that is perhaps adopted from the MTV reality TV show *Catfish*.

> *Catfish (verb): To pretend to be someone you're not online by posting false information, such as someone else's pictures, on social media sites.*
>
> – MTV's *Catfish* website [8]

People in the study used the term to describe a range of behaviors from the relatively innocuous – such as using the profile photo of a more attractive cousin as your Instagram profile – that would merely surprise people when they met in person, to the potentially life threatening. Impersonating someone on Facebook to become "friends" with a target was viewed as common. One technique is to use a photo of someone in the community that the target knows only by sight, and add a message that "It was nice to see you in church" with the friend request. One participant explained that the risk is of clicking on a wrong link – that is, accepting a Facebook friend request from a catfisher – is that the police then have access to your posts and your friends. The police chief of Brownsville, where several of the participants who discussed catfishing lived, recently shared his pride in the precinct's Facebook policing program with the *New York Times* [9]. Similarly, *The Verge* reported how one Harlem teenager's Facebook likes of allegedly gang-related photos led to a sentence of 20 years in Rikers Island prison [10].

Online surveillance by corporations was seen as "creepy," but without the immediate consequences for harm of being catfished. Participants shared examples of kinds of corporate surveillance that they found disturbing, such as targeted ads following people across devices. One of our interviews took place at a Dunkin Donuts near the participant's house in Harlem. She's a big fan of Dunkin Donuts, and uses the DD mobile app. It's a digital version of the loyalty punch cards that give a free cup of coffee after so many purchases. Saving money is a strong motivator, and several of the participants used fast food apps for other stores like McDonald's as well. Even though these apps are common,[1] nobody mentioned privacy concerns with them. One area where users might identify concerns with an app's behavior is in the permissions it requests upon install. The Dunkin' Donuts Android app permissions include location tracking, reading the user's address book, editing text messages, deleting the contents of storage, and preventing device from sleeping [12]. For someone with an older handset with limited battery life, an app that prevents sleeping could cause someone to miss a crucial work-related call. App developers may have legitimate, user-centered reasons for requiring these permissions – or our study participants may unknowingly giving sensitive personal information to these corporations in exchange for their popular loyalty-card benefits.

Summary of Findings

The interplay of the physical, social, cultural, and technological systems has created an environment of inevitable surveillance for the low-income African-Americans who participated in our study. They have no safe harbor from surveillance at work, home, or in public. They work in jobs where their phones are regularly out of their physical control. Economics drive them into living situations with people they don't trust and who have regular opportunities to gain access to their phones. This leaves their devices open to a host of physical-security concerns, particularly shoulder surfing.

The implications of the phone as a surveilled space extend beyond the physical and into the digital as well. Family plans and social engineering can give people access to participants' private messages and location data through the carrier. Participants had a renters' mindset: carriers own their devices, and therefore inevitably have access to all data on them, including personal content and messages. Because most of them had older Android handsets with limited storage space, they were continually worried the carriers would push software to their phones that would break them. When a phone is critical for employment and well-being, people aren't willing to experiment with apps that might make their phone crash or "glitch." This points to a systemic barrier to experimentation with emerging open-source apps.

Finally, discussion of messaging behavior led to shared experiences of surveillance by "the feds," who "catfish" people in Facebook. Governmental surveillance was a more pressing concern, with corporate surveillance relegated to the position of "creepy." Even though loyalty-card apps with questionable permissions were used by some participants, they raised no concerns about in-app surveillance in our discussion.

[1] As a small sample, English-language apps made by McDonald's, Pizza Hut, Domino's Pizza, Papa John Pizza, and Dunkin' Donuts have each been downloaded 5-10 million times from the Play Store [11]. Many companies have apps tailored to different countries, and there are also many third-party apps advertising discounts for a variety of fast-food restaurant chains.

Conclusion

Our research points to significant gaps between the priorities of our low-income African-American participants and those of the security and privacy communities of academia, industry, and civil society. First, our participants believed that governmental surveillance was inevitable, which stands in contrast to the efforts of activists, open-source developers, and a host of policy experts. Second, physical-device security is considered a "solved problem" from a technical perspective, but was tremendously important to participants, and had notable influence on their messaging behaviors.

These gaps point to a most pressing problem for those who seek to encourage adoption of apps with strong privacy protection. How do we explain the value of a secure-messaging app? What does it provide beyond what alternatives like Snapchat offer? What real-world problem does it solve? In an environment where surveillance is seen as inevitable and shoulder-surfing is the real threat, how do we make the case that end-to-end encryption matters?

The original plan for this study was to have participants download a messaging app with end-to-end encryption, such as Signal or Threema, onto their phones, exchange messages during the interview, and give feedback about the user experience. (As previously described, this proved too burdensome because it would have required participants to remove existing apps to make room on their phones.) We also brought a phone with Signal installed, imagining participants could alternatively use that to message with us. However, we only made it through the preliminary step in this process – getting feedback on the app's listing in the app store – because the app description triggered such rich conversation. Participants questioned the motivation behind the app. They believed the phrase "open source" in the description meant messages were publicly available somewhere, and they could not reconcile that with the app's security claims. App listings contained illustrative screenshots that featured old messages still visible in the chat history, which did not match participants' threat models. The pressing threat of shoulder-surfing and physical security made time-limited messages seem more secure to participants than written claims about encryption.

Overall, the app store descriptions did not compel people to download the app because they were confusing and off-putting. One participant bluntly asked, "Is this secure, or is it regular?".

Initial design directions

Building on insights from our study, the following initial design directions could improve existing secure communication apps' appeal with our participants:

- Re-design app store descriptions to include a clearer value proposition
- Consider supporting ephemeral communication, where messages are automatically deleted from the chat history
- Explore use of "blocking" as a term for limiting unwanted access history after a certain amount of time

As an example of clear value proposition, SnapChat has elements worthy of emulating. Their use of language to describe the benefits of ephemeral communication has been extraordinarily successful in communicating value to end users. Multiple participants repeated SnapChat's descriptions of "disappearing" messages practically verbatim. When physical security is the primary concern, SnapChat's claims – although technically insecure in relation to many threat models – meet the participants' expectations.

A related direction is to explore "blocking" as language for privacy preservation, both in the app store description, and in the words in the interface. Participants used "blocking" spontaneously to talk about phone numbers they had blocked (in some cases multiple screens worth), and used block lists in messaging apps such as Twitter. Extending the language of blocking to app creators, carriers, or governments could clarify the value of encryption. Our initial conversations using blocking to describe shielding content from an adversary were promising.

Clarifying the value proposition of secure communication apps to include blocking and to emphasize time-limited messages might motivate our participants to voluntarily select and use secure communication apps. We heard our participants' wishes for more privacy in their communication, and look forward to working with people with similar concerns to prototype better software that meets their needs. One challenge with involving low-income people in longitudinal, in-situ experimentation is that they may be (quite reasonably) unwilling to install experimental software on their devices. With the phone a vital lifeline for economic and emotional well-being, installing potentially-buggy software that may cause an older phone with out of date system software to crash is too risky for some of our participants.

We want to make our participants' stories accessible to members of the technical community who may not have first-hand experience with mobile messaging in a context like this one. The findings shared here are a small window into broader set of lived experiences, with relevance far beyond Harlem and Brownsville. These insights can be a catalyst for designing privacy-preserving software that meet the needs of a diverse, global audience, and that makes end-to-end encryption accessible to all.

Resources

Simply Secure shares non-code resources that help software teams working on privacy-preserving projects. Visit the Research directory of https://github.com/simplysecure for assets related to this work, including:

- Screener
- Interview Guide
- Participant Bill of Rights
- Consent Form
- Model Release

Bibliography

[1] Browne, Simone, *Dark Matters: On the Surveillance of Blackness*. Duke University Press, 2015.

[2] George, Joseph, “Exclusive: Feds Regularly Monitored Black Lives Matter Since Ferguson”. *The Intercept*, July, 24, 2014.
https://theintercept.com/2015/07/24/documents-show-department-homeland-security-monitoring-black-lives-matter-since-ferguson/ Accessed April 6, 2016.

[3] Second Muse, “Understanding Internet Freedom: The Tibetan Exile Community”. September 2014.
http://internetfreedom.secondmuse.com/wp-content/uploads/2015/02/if_dharamsala_low.pdf

[4] McLaughlin, Jenna, “The FBI vs Apple Debate Just Got Less White”. *The Intercept*, March 8, 2016.
https://theintercept.com/2016/03/08/the-fbi-vs-apple-debate-just-got-less-white/ Accessed April 19, 2016.

[5] Madden, Mary and Rainie, Lee, “Americans’ Attitudes About Privacy, Security, and Surveillance”. Pew Research Center Reports, May 2015.
http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/

[6] Stanton, Brandon, *Humans of New York*. https://www.instagram.com/humansofny, Accessed April 21, 2016.

[7] Katz, Lawrence F and Krueger, Alan B. "The Rise and Nature of Alternative Work Arrangements in the United States, 1995-2015”, March 2016.
http://scholar.harvard.edu/files/lkatz/files/katz_krueger_cws_v3.pdf Accessed April 21, 2016.

[8] MTV. Catfish: The TV Show, http://www.mtv.com/shows/catfish-the-tv-show Accessed April 20, 2016.

[9] Secret, Mosi. “On the Brink in Brownsville”. *The New York Times*, May 1, 2014.
http://www.nytimes.com/2014/05/04/magazine/on-the-brink-in-brownsville.html Accessed April 7, 2016

[10] Popper, Ben. “How the NYPD is Using Social Media to put Harlem Teens Behind Bars”. *The Verge*, December 10, 2014.
http://www.theverge.com/2014/12/10/7341077/nypd-harlem-crews-social-media-rikers-prison Accessed April 7, 2015.

[11] Statistics drawn from individual apps’ Play Store listings on April 21, 2016.
https://play.google.com/store/apps

[12] Permissions for version Version 3.8.3 of the Dunkin’ Donuts app in the Google Play Store.
https://play.google.com/store/apps/details?id=com.skcc.corfire.dd Accessed April 7, 2016.