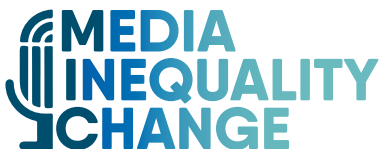


CELL PHONES, SECURITY AND SOCIAL CAPITAL:

EXAMINING HOW PERCEPTIONS OF
DATA PRIVACY VIOLATIONS AMONG
CELL-MOSTLY INTERNET USERS
IMPACT ATTITUDES AND BEHAVIOR

Jan Fernback and Gwen Shaffer



About MIC



The Media, Inequality & Change (MIC) Center is a collaboration between the University of Pennsylvania's Annenberg School and Rutgers University's School of Communication and Information. The Center explores the intersections between media, democracy, technology, policy, and social justice. MIC produces engaged research and analysis while collaborating with community leaders to help support activist initiatives and policy interventions. The Center's objective is to develop a local-to-national strategy that focuses on communication issues important to local communities and social movements in the region, while also addressing how these local issues intersect with national and international policy challenges.

About the Authors

Jan Fernback, PhD, is Associate Professor of Media Studies in the Klein College of Media and Communication at Temple University. Her current work examines issues of privacy and surveillance online and in mobile technologies, the impact of information/communication technologies on urban revitalization efforts, institutional uses of ICTs, ethics and virtual assistants, and the meaning of virtual community in contemporary culture. She is an award-winning teacher, the creator of a communication pedagogy curriculum for Ph.D. students, and author of *Teaching Communication and Media Studies: Pedagogy and Practice*, published by Routledge. Her work has been published in *New Media & Society*, *Information, Communication & Society*, and *Communication, Capitalism & Critique*, among other journals and edited books.

Gwen Shaffer, PhD, is an associate professor in the Department of Journalism and Public Relations at California State University Long Beach. Her research focuses on telecommunications policy analysis, and examines digital inequality, data privacy, and social exclusion in the informational age. Recent projects investigate efforts by state lawmakers to deregulate VoIP services, and the potential for community WiFi networks to help close the digital divide. The National Science Foundation and the John Randolph and Dora Haynes Foundation have funded Shaffer's research. Her work has been published in *Media, Culture & Society*; the *Journal of Information Policy*; *First Monday*; and the Association for Computing Machinery's *Transactions on Internet Technology*, among other journals and edited books. Shaffer chairs the City of Long Beach's Technology and Innovation Commission, which advises the mayor and City Council on relevant policy issues. Prior to joining the faculty at CSULB, she was a postdoctoral fellow in the Department of Computer Science at UC, Irvine.

About the Report

This research highlights the intersection between emerging forms of digital inequity and long-standing socio-economic injustices. The authors illustrate how low-income Americans who rely on smartphones to access the internet are aware of frequent surveillance by corporations, social media platforms and the government. In an effort to maintain data privacy, they sometimes modify online activities in ways that harm personal relationships and force them to forego professional opportunities. Study participants, generally, seemed resigned to their status as having little power and minimal social capital.

Table of Contents

Executive Summary	4
Introduction	5
Context for the research	7
Policy landscape	10
Methodology	11
Findings	12
Concerns about security and privacy	13
Practices	13
Trust	18
Recommendations for cell-mostly internet users	20
Regulatory responsibilities	20
Recommendations for policymakers	22
Willingness to act	22
Recommendations for tech companies, mobile phone carriers, and consumer privacy advocates	23
Conclusion	24
Appendix A	25
Appendix B	26
Appendix C	26

Executive Summary

This project details the kinds of online privacy tradeoffs that disproportionately impact cell-mostly internet users. It draws connections between and builds upon two distinct bodies of research that address technology-driven inequalities, both of which have policy implications. First, economically disadvantaged individuals, Hispanics, and African Americans are significantly more likely to rely on phones to access the internet, compared to wealthier, white Americans. Similarly, people of color are heavier users of social media apps compared to white Americans. Second, mobile internet use, mobile apps, and cell phones themselves leak significantly more device-specific data compared to accessing websites on a computer. In light of these combined realities, we wanted to examine the kinds of online privacy tradeoffs that disproportionately impact cell mostly internet users and, by extension, economically disadvantaged Americans and people of color.

We partnered with three community-based organizations in both Long Beach, Calif., and Philadelphia to recruit 79 cell-mostly internet users for focus groups. We posed three research questions. First, how do cell-mostly internet users—who tend to live in economically marginalized communities—articulate the perceived risk factors affecting their mobile phone data practices? In other words, how do they conceptualize data privacy? Second, we explored to what extent cell-mostly internet users considered mobile privacy breaches to be discriminatory or unjust. Finally, we asked study participants how they alter their behavior or pass up opportunities due to privacy concerns.

Some focus group participants reported that, in an effort to maintain data privacy, they modify online activities in ways that harm personal relationships and force them to forego job opportunities. We find these admissions particularly troubling. Study participants, largely, seemed resigned to their status as having little power and minimal social capital. The project findings shine light on an increasingly serious problem of digital life—the inequities exacerbated by data insecurity that are experienced by all individuals but are more salient among those living in economic precarity.

A surprising theme that emerged from these conversations is that nearly all the cell-mostly internet users interviewed said they believe that individual smartphone users—as opposed to the corporations, social media platforms and government agencies that track their online activities—bear responsibility for safeguarding private data.

Focus group discussions revealed that:

- Study participants were generally aware that both governments and corporations collect, store, and use mobile data.
- Few participants said they would abandon highly-invasive mobile apps, such as the Google search engine and Gmail, for more secure alternatives.
- Only about 10% of study participants used iPhones, which are known to provide a more secure ecosystem, compared to Android phones.
- Study participants are on their phones “24/7,” “a few times an hour” and one even commented that the phone “is a part of me.”

These anecdotes are supported by the app tracker data we collected from 14 Android users who installed App Usage for two weeks. The data showed:

- Study participants typically used phone apps for about six hours per day.
- Apps ran (and collected data) for as many as 22 hours on some days.
- Participants spent time each day on multiple apps—including YouTube, Facebook and Google Chrome—that request permission to access contacts, web browsing history, SD cards, photos, text messages, microphones and more.

Introduction

Tanya, a 30-something African American woman who lives in Philadelphia, refuses to fill out online applications for jobs or credit cards. She doesn't own a computer and exclusively uses her phone to go online. "I'm suspicious of that process...giving out my name, my number," Tanya said. "It is very inconvenient for me to not be able to apply for jobs on my phone, and I probably am missing opportunities."

Shelly, a formerly homeless woman in her 50s who lives in Philadelphia and doesn't use a computer, is afraid to make purchases on her cell phone. "I've seen the LifeLock commercials and I know people will steal your information off the phone. That's true," she said.

Karla, another Philadelphia woman in her 50s who lives in transitional housing, worries about data collection by social media platforms. However, without a car or cash, posting to Facebook is a necessity. "I use Facebook because it is the only way I can be in touch with my family," Karla said. Jazmin, a Hispanic woman who lives in Long Beach, Calif., voiced similar concerns about social media platforms. In fact, she deleted Facebook from her phone after hearing about the company's repeated privacy violations. "But I needed to use it, so I installed it again."

The sentiments expressed by these cell-mostly internet users¹ are not unique. We facilitated focus group discussions with 79 people in Philadelphia and Long Beach, all of whom rely on their phones to go online. Through participant observation, we also gained insight into the most popular apps for cell-mostly internet users and how much time they spend engaging with them. This white paper details the kinds of online privacy tradeoffs that disproportionately impact cell mostly internet users—who are likely to be Black, Hispanic or low-income. Nearly all study participants shared stories of relinquishing their data privacy, which we consider to be a basic civil right, in exchange for the ability to access online services and platforms. Many people shared anecdotes about forgoing opportunities in an attempt to

maintain data privacy. The research finds that members of disadvantaged urban communities who rely on mobile phones to access the internet and frequently use mobile apps, may be disproportionately subjected to privacy violations—sometimes forcing them to alter online behavior in ways that harm personal relationships and limit prospective employment. And, as Virginia Eubanks² has articulated, Americans who rely on public benefits are often the "canaries in the coalmine" when it comes to data collection. This is because the algorithms and digital tools initially used to track marginalized Americans ultimately become mainstream. For Eubanks,³ the algorithmic bias was personal. After her domestic partner was violently attacked, their insurance company denied them coverage based on an algorithm that flagged them for a fraud investigation based on the relative newness of their policy. Eubanks explains that marginalized groups are subject to extra scrutiny based on the large amounts of data collected on them as they apply for public benefits or make health care claims. These populations are thus easier to surveil, easier to track, and harder to protect.

An unexpected finding is that nearly all the interviewees said they believe individual smartphone users—as opposed to tech platforms, government and corporations—bear responsibility for safeguarding private data. The study participants we interviewed, generally, failed to recognize critical structural issues that enable a surveillance economy to thrive. This self-blame for data privacy violations may partially explain why victims of data breaches do not vociferously demand that policymakers and corporations implement data-protective policies.

1 The names of study participants have been changed to ensure their anonymity.

2 Eubanks, V. (2018, October 23). *Automating Inequality: How high-tech tools profile, police, and punish the poor*. Talk given at the Berkman Klein Center for Internet & Society. Retrieved from <http://opentranscripts.org/transcript/automating-inequality/>

3 Eubanks, V. (2017). *Automating Inequality: How high-tech tools profile, police, and punish the poor*. New York: St. Martin's Press.

Survey data collected by the Pew Research Center,⁴ as well as related research by the Data & Society Research Institute,⁵ provide useful statistics about mobile technology habits. However, numbers lack context and detail, and do not allow respondents to explain choices or offer perspectives in their own words. Similarly, it is difficult to obtain survey data about the values that compete with privacy concerns, such as convenience, cost and time. By contrast, our study findings are based on empirical evidence provided during interviews with disadvantaged urban residents who exclusively access the internet from their smartphones. By facilitating small focus groups—some with as few as four participants—we were able to collect nuanced qualitative data, and to humanize the impact of privacy breaches through informants' lived experiences. We also analyzed mobile phone usage data collected from 14 cell-mostly internet users. These participants installed a mobile app tracker and shared the data during a two-week span.

Community input and collaboration are fundamental to this project. We partnered with Downtown Associated Youth Services (DAYS), a non-profit agency that provides free educational programming and youth development activities for low-income, underserved families in Long Beach. We also partnered with Pathways to Housing PA, a Philadelphia-based non-profit that strives to end homelessness through mental and physical health treatment, education, and employment training. Finally, Philadelphia FIGHT staff helped us recruit focus group participants. This organization provides comprehensive medical care to low-income people, along with consumer education, research, advocacy, and social services to people living with HIV and at-risk individuals. These organizations were ideal partners because they each work with populations most likely to rely on cell phones for accessing the internet: members of the Hispanic and African American communities, and low-income residents.

4 Pew Research Center (2018, February 5). Mobile fact sheet. Retrieved from <http://www.pewinternet.org/fact-sheet/mobile/>.

5 Madden, M. (2017). Privacy, Security and Digital Inequality. Data & Society Research Institute.

Context for the research

This project draws connections between and builds upon two distinct bodies of research that address technology-driven inequalities with policy implications. First, economically disadvantaged individuals, Hispanics, and African Americans are significantly more likely to rely on phones to access the internet, compared to wealthier, white Americans.⁶ People of color are also heavier users of social media apps compared to white Americans. Second, mobile internet use, mobile apps, and cell phones themselves leak substantially more device-specific data compared to accessing websites on a computer.^{7,8} Because of these combined realities, marginalized Americans who rely on cell phones for internet access are disproportionately impacted by online privacy violations from corporations, social media platforms, and government.

Increasingly, all U.S. adults are likely to access the internet on their smartphones. The reality, however, is that skin color and income largely determine whether someone depends on a mobile device to go online. Specifically, 25% of Hispanics own a smartphone but lack a home broadband connection. And nearly 23% of African Americans rely on their mobile devices to get online. By contrast, 12% of white Americans can be characterized as cell-phone dependent.⁹ The disparity in broadband access is evident when it comes to low-income adults, regardless of race. Specifically, 26% of U.S. adults earning less than \$30,000 per year lack a home broadband connection but own a smartphone,

while just 6% of Americans earning \$75,000 or more depend on their phones for internet access.¹⁰

These statistics are even more powerful when combined with previous study findings that mobile internet use, mobile apps, and cell phones themselves leak significantly more device-specific data compared to accessing websites on a computer. When people access the internet using a mobile device, with an Android operating system or iOS, they leave behind an average of 32 “digital traces”—from their browser histories and phone numbers, to their geo-locations and photos. This compares to 14 traces accumulated by Mac users and 24 by Windows users.¹¹

Surveillance: The use of apps represents a major source of vulnerability for marginalized populations; they are at the heart of dialogues about online privacy.^{12,13} Facebook, Twitter, Yelp, and Instagram are among the mobile platforms that send the names, email addresses and potentially phone numbers from a device’s internal address book to the apps’ own servers.¹⁴ WhatsApp, Messenger and similar platforms collect and share consumer data. Analysis of more than 1 million apps in the Google Play store found that, on average, apps request 5 permissions.¹⁵

For those living in urban areas, government surveillance is an every day occurrence.¹⁶ Surveillance by cell-site simulators and social media monitoring, for example,

6 Pew Research Center, *ibid.*

7 Papadopoulos, P., Diamantaris, M., Papadopoulos, P., Petsas, T., Ioannidis, S., & Markatos, E. (2017, April). *The long-standing privacy debate: Mobile websites vs. mobile apps*. International World Wide Web Conference, Perth, Australia. Retrieved from http://sharcs-project.eu/m/filer_public/91/b3/91b327e6-1472-45e3-b0bc-ca20bdb0fe75/mobile_websites_vs_mobile_apps_-_www2017.pdf.

8 Me and My Shadow (2017). *Trace my shadow*. Retrieved from <https://myshadow.org/trace-my-shadow>.

9 Anderson, M. (June 13, 2019). *Mobile Technology and Home Broadband 2019*. Pew Research Center. <https://www.pewinternet.org/2019/06/13/mobile-technology-and-home-broadband-2019/>.

10 *Ibid.*

11 Me and My Shadow (2017).

12 Pew Research Center (2018, February 5). Internet/broadband fact sheet. Retrieved from <http://www.pewinternet.org/fact-sheet/internet-broadband/>

13 Atkinson, M. (2015, November 10). Apps permissions in the Google Play Store. Pew Research Center. Retrieved from <https://www.pewinternet.org/2015/11/10/apps-permissions-in-the-google-play-store>

14 Van Grove, J. (2012, February 14). Your address book is mine: Many iPhone apps take your data. *VentureBeat*. Retrieved from <http://venturebeat.com/2012/02/14/iphone-address-book>

15 Pew Research Center (2015).

16 Gray, D. (2017). *The Fourth Amendment in an age of surveillance* (p. 37). Cambridge: Cambridge University Press.

ostensibly target criminals and terrorists. However, these law enforcement techniques disproportionately impact people of color. Losing the expectation of privacy can markedly suppress civic engagement¹⁷ and, by extension, diminish social capital.¹⁸

Smartphone security vulnerabilities: The premise of this project is supported by evidence that mobile phone apps leak “significantly more device-specific data”¹⁹ to advertisers and data analytics firms, compared to websites. About 69% of web browsers tested during a 2017 study leaked data to an average of 5 third-party trackers. By comparison, nearly 94% of Android apps tested leaked data to an average of 11.7 third-party trackers. The types of data leaked, including nearby

access points and details about other apps running on the phone, may allow tracking domains to infer user interests, gender, even behavioral patterns. These leaks enable third parties to correlate eponymous with anonymous sessions.²⁰ Additionally, nearly 58% of apps tested leaked the “Android ID” identifier, while web browsers typically lack access to these data.

Cell phone files tend to be more personally revealing than those found on a computer—encompassing photos, videos, voicemails, text messages, geo-location data and contacts. Yet, just 14% of smartphone owners install an antivirus program on their device, and 33% take no steps to secure data on their devices.²¹ Consequently, mobile devices are more vulnerable to privacy breaches than computers when accessing the internet.²²

Currently no federal privacy laws attending to

17 Schneier, B. (2006, May 18). The eternal value of privacy. *Wired*. Retrieved from https://www.schneier.com/essays/archives/2006/05/the_eternal_value_of.html

18 Davilo, A. and Mora, M. (2007). *An assessment of civic engagement and education attainment*. The Center for Information & Research on Civic Learning & Engagement. Retrieved from http://www.civicyouth.org/PopUps/Fact-Sheets/FS_Mora.Davila.pdf

19 Papadopoulos, et al. (2017), (p. 6)

20 *Ibid*

21 Consumer Reports (2014). Smartphone thefts rose to 3.1 million in 2013. Retrieved from <http://www.consumerreports.org/cro/news/2014/04/smart-phone-thefts-rose-to-3-1-million-last-year/index.htm>

22 Federal Trade Commission (2018, February). *Mobile security updates: Understanding the issues*. Retrieved from <https://perma.cc/A4FZ-YCMT>

Table A. The following table identifies features and functions belonging to both mobile devices and PCs and shows how cell-mostly internet users' privacy is at greater risk.

Function/Feature	PC	Mobile Phone
Leaking data to third-party trackers	≈ 69% of tested browsers leak to 5 advertisers, data analytics firms, etc.	≈ 94% of tested Android apps leak to 12 advertisers, data analytics firms, etc.
Attack surface	Communicates wirelessly over Wi-Fi	Communicates wirelessly over WiFi, NBT and Bluetooth
Security updates	Well-supported updates sent quickly	Updates sent slower especially for Android devices; some phone manufacturers drop support 1-2 years after their initial release
Web browsing	Potentially dangerous sites are routinely flagged	Potentially dangerous sites less effectively identified (screen size a factor)
Anti-virus software	Conventional anti-virus software programs partially rely on pattern detection to ID malicious files	Anti-virus software cannot depend on pattern detection to ID malicious files; pattern detection ports poorly to mobile devices
Firewalls	Firewalls commonly protect PC networks	Firewalls not built into mobile phones
Device ID leaks	Web browsers typically do not have access to this data	≈ 58% of tested apps leak "Android ID" identifier
Apps and websites	Social media platforms lack access to internal address book, email contacts and location when accessed from a PC	Facebook, Twitter, Instagram, and Yelp send names, email addresses and phone numbers from a device's address book to apps' own servers
Hardware identification	End user can avoid most browser-based tracking with minimal effort; cookies and local shared objects can be deleted	Mobile apps use hardware IDs that cannot be deleted or reset. Third parties that track and store end user network traffic information can associate it with the end user device indefinitely
Device down-time	PCs often turned off or in sleep mode	Mobile devices typically on 24/7, giving access to bots and hackers
Passing via public routers	PCs that use public routers to go online require a password	Public routers often do not require passwords from smartphones—enabling data between a phone and the router to be sniffed
Government surveillance	Via data collection agreements with ISPs, law enforcement agencies collect browser history and email exchanges	Via data collection agreements with wireless carriers, law enforcement agencies collect browser history, email exchanges, address books, text messages, geolocation data, and photos; police use cell site simulators to collect internet, text and voice communications; social media monitoring apps reveal geolocation data and platform activity

Policy landscape

consumer data tracking and sale exist. The U.S. Federal Trade Commission (FTC) is charged with protecting consumer data privacy but has nominal authority to influence or uphold privacy legislation. The Electronic Communications Privacy Act of 1986, which specified limits on government access to computer communication less than six months old, is outdated and provides minimal consumer data protections.²³ The Privacy Act of 1974 oversees individual data kept by the federal government and identifies measures for the collection, amendment of, access to, and dissemination of those data. However, government agencies engaged in law enforcement do not have to comply with this statute.²⁴ Federal privacy laws governing private companies' use of consumer data are fragmentary.²⁵ For example, under the Fair Credit Reporting Act (FCRA), individuals have no federal remedy for modifying inaccurate or suspect data used for "people search" or for marketing purposes not covered by the FCRA.²⁶ The FTC developed fair information principles in 1977, but Congress never codified them into law. As a result, the commission lacks authority to strongly enforce privacy rules.

By contrast, the EU General Data Protection Regulation (GDPR), enacted in 2018, ensures equilateral data privacy laws across EU nations and aims to provide more individual control over personal data. The law enumerates citizen data privacy rights and provides modes for redress of data privacy grievances.²⁷ Under the GDPR, businesses must anonymize data, permit user consent, and disclose occurrences of data collection.²⁸

No similar laws exist at the federal level in the U.S., and numerous attempts to bring data privacy legislation for a vote in Congress have failed.

However, state-level laws are gaining traction. The California Consumer Privacy Act (CCPA)²⁹ is meant to give residents of the state true control over the information businesses collect on them, and imposes penalties on businesses that fail to comply. Privacy experts characterize this law, scheduled to take effect Jan. 1, 2020, as the most stringent data privacy regulation in the United States. The CCPA is sparking both legal and policy debates over whether California has the right to set rules that could become de facto national standards, or whether federal rules preempt California's move.³⁰ Powerful industry groups, including the Internet Association³¹ and the Chamber of Commerce,³² are pushing Congress to adopt a privacy framework that would be applied consistently nationwide and that would supercede state consumer privacy laws. These stakeholders contend that a patchwork of conflicting state rules would create regulatory uncertainty and confusion for industry.

The researchers interviewed a total of 79 cell-mostly

23 Center for Democracy and Technology, *ECPA Reform*. <https://cdt.org/issue/security-surveillance/ecpa-reform/>

24 Electronic Privacy Information Center (2019). *The Privacy Act of 1974*. <https://epic.org/privacy/1974act/>

25 Government Accounting Office (2013, September). *Information resellers: Consumer privacy framework needs to reflect changes in technology and the marketplace*. GAO-13-663 *Information Resellers*. <http://www.gao.gov/assets/660/658151.pdf>

26 *Ibid*

27 European Commission. *Protection of Personal Data*. https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/know-your-rights/freedoms/protection-personal-data_en

28 GDPR Key Changes. <https://eugdpr.org/the-regulation/>

29 SB 1121/California Consumer Privacy Act full text, https://leginfo.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121

30 WilmerHale (2018, July 2). *California enacts sweeping consumer privacy law*. https://www.wilmerhale.com/en/insights/client-alerts/20180702-california-enacts-sweeping-consumer-privacy-law?utm_source=Mondaq&utm_medium=syndication&utm_campaign=inter-article-link

31 Internet Association (2018, November 30). *IA privacy principles for a modern national regulatory framework*. https://internetassociation.org/files/ia_privacy-principles-for-a-modern-national-regulatory-framework_full-doc/

32 U.S. Chamber of Commerce (2019). *U.S. Chamber of Commerce privacy principles*. https://www.uschamber.com/sites/default/files/9.6.18_us_chamber_-_ctec_privacy_principles.pdf

Methodology

internet users. Specifically, 36 people participated in four 60-90-minute focus groups hosted by DAYS Long Beach in January 2019. Fourteen people participated in two focus groups hosted by Pathways to Housing PA in February 2019. Sixteen people recruited through Philadelphia FIGHT participated in two focus groups held at Temple University in February and March 2019. Finally, our findings were informed by discussions we had with 12 people during pilot focus groups in May 2017 at Centro C.H.A., a non-profit social service agency that advocates for the well-being of low-income, Hispanic families in Long Beach.

We asked participants about general mobile phone practices; their knowledge of data tracking and leakage; their attitudes toward mobile data privacy; their perceptions of data discrimination; factors that influence which websites they visit and which apps they access via their phones; and their ideas about responsibility for phone data security.

To further understand the mobile phone practices of

the disadvantaged community members at the center of this project, we recruited 14 study participants to install App Usage. This free app enables Android phone users to track how much time they spend using their mobile phones, including a breakdown by specific app (i.e. Instagram, YouTube, Waze, voice calls, Chrome, Spotify). Study participants in both Long Beach and Philadelphia provided us with detailed reports on phone usage over a 2-week period. We recognize the irony of asking participants in a mobile phone privacy study to install a usage tracking app. Significantly, however, the reports generated by these apps do not reveal the content of social media posts, websites visited, or phone numbers dialed. The reports, in the form of CSV files, exclusively detail how much time a mobile phone user engaged in specific activities. We realize using a phone usage tracking app might influence online behavior, but software that runs in the background was the least intrusive and most precise data collection tool available.

Two main areas of inquiry frame our findings. First, a

Table B. Participants represented a range of ages, racial/ethnic identities and languages spoken.

Age	Number of Participants					
18-24 years old	26					
25-31 years old	10					
32-40 years old	11					
41-50 years old	11					
51-60 years old	15					
61 years or older	4					
Racial/ethnic identity (self-identified)*	White	Black/African American	Latino/Hispanic	Asian	Other	Declined to state
Number of participants	5	20	46	3	2	1
Language spoken**	Spanish only		English only		Bilingual	
	18		26		20	

* Forty participants were female and 37 were male. Two participants did not identify racial/ethnic identity or gender.

** We did not collect language data for the 12 people who participated in the May 2017 pilot study.

Findings

theoretical position grounded in science and technology studies (STS) considers technologies “as value-laden social processes taking place in specific contexts—interactively shaped by, and in turn shaping, the human values reflected in cultural, political, and economic institutions.”³³ Additionally, our interpretation of STS is informed by communication theory, which considers technology design and user consumption practices to engage with issues of social inequality.³⁴ STS interrogates the ways in which technology is linked to socio-democratic principles and values, including fundamental privacy rights. Second, social capital theory provides a framework for developing policy suggestions aimed at empowering mobile phone users in disadvantaged neighborhoods. Our framework examines how power, as conceived and enacted, influences socio-technical realities.

The study’s key findings indicate that cell-mostly users are generally aware that both governments and corporations collect, store, and use their cell phone data. They were surprised, however, to learn the extent of these surveillance practices. Many seemed resigned

to their status as having little power, little social capital, and little hope that anything will change at either the governmental or corporate levels. Some STS-related theories argue that users actively establish meaning over time and in context; the study participants show a complex negotiation of meanings in different contexts.

Participants felt so connected to their phones, overall, that they referred to them as “lifelines” and “my whole life.” But this attachment is moderated by antipathy in that they sometimes regard the phone as an open book of sorts into their lives. Some say the government tracks them through their phones, but they engage in so many activities (e.g., shopping, banking, social media) that they experience, not unlike many people, tensions between feeling trapped by the phone but liberated by how it allows them to participate in modern society.

Here, we present the study findings thematically. Major themes emerging from the data include: Concerns about security and privacy (which is comprised of two sub-themes—trust and practices); regulatory responsibilities; and willingness to act. The following sections explore these themes in detail.

Fewer than 10% of the study participants used iPhones,

33 Ibid, p. 3.

34 Boczkowski, P., & Lievrouw, L. A. (2008). Bridging STS and communication studies: Scholarship on media and information technologies. In E.J. Hackett, O. Amsterdamska, M. Lynch, & J. Wajcman (Eds.), *The handbook of science and technology studies*, third edition, pp. 949-977.

Concerns about security and privacy

which are known to provide users with a more secure ecosystem, compared to Android phones.^{35,36} Apple uses hardware innovations to thwart external hacking and imposes its privacy protections onto third-party app developers. The company also uses differential privacy (a statistical technique) to scramble the data it collects on users, making it impossible to identify people personally.³⁷ By contrast, more malware is written for Android phones and Google's business model depends on the company acquiring as much data about users as possible.³⁸ Lower income users are effectively steered toward Android

models due to their lower price-point. Android phones also present fewer barriers to entry into cell phone usage since most free and government-subsidized phones are Android based. Disadvantaged users are therefore more vulnerable to privacy violations in the form of "update lag" since updates must be customized to each carrier or device maker before they're offered to users. Android phone manufacturers extensively test Google updates, delaying installation of software patches.³⁹ These market realities provide context for our study findings, which indicate that while some participants are concerned about their cell phone data privacy, even those users are reluctant to take much action to secure their data. As one young participant stated, "I don't post anything negative on social media, so I am safe."

35 Grothaus, M. (2018, September 13). Forget the new iPhones: Apple's best product is now privacy. Retrieved from <https://www.fastcompany.com/90236195/forget-the-new-iphones-apples-best-product-is-now-privacy>

36 Nield, David (2018, February 16). Why Choosing Between Android and iOS Still Matters. Retrieved from <https://gizmodo.com/why-choosing-between-android-and-ios-still-matters-1822976032>

37 Grothaus (2018).

38 Nield (2018).

39 Federal Trade Commission (2016).

Practices

Study participants reported being on their phones "24/7," "a few times an hour" and "15 to 20 times a day." Even so, they tended either to not worry much about cell phone data privacy or to be reconciled to feeling little control over data. Other participants reported feeling powerless to curtail data collection. These attitudes are evident in the practices in which they engage while online, based on the app tracker data we collected from 14 Android phone users. For instance, one of the study participants who provided data collected through App Usage spent nearly 70 hours viewing YouTube on his phone during the 2-week period tracked. That averages out to five

hours a day when YouTube is actively accessing this person's contacts, photos, location, the contents of his USB storage device and more. Two study participants viewed YouTube on their phones for 58 hours and 37 hours respectively; 10 other participants used the app for periods ranging from 25 hours to 35 minutes during their 2-week tracking periods. Overall, YouTube was the app most frequently used most by all study participants combined, with 12 phones accessing it for about 234 hours during the 2-week tracking period.

Table C. Permissions automatically granted by phone users when they download YouTube’s mobile app.

YouTube phone permissions (partial list)	
Identity find accounts on the device add or remove accounts	Storage read the contents of your USB storage modify or delete the contents of your USB storage
Contacts find accounts on the device read your contacts	Microphone record audio
Location approximate location (network-based) precise location (GPS/network-based)	Wi-Fi connection information view Wi-Fi connections
Phone read phone status and identity	Device ID & call information read phone status and identity
Photos/Media/Files read the contents of your USB storage modify or delete the contents of your USB storage	Other manage document storage receive data from Internet view configured accounts YouTube usernames YouTube view network connections measure app storage space
Camera take pictures and videos	
Contacts find accounts on the device	

The sheer number of apps installed by some study participants is also worth noting, given the multiple types of data each piece of software collects. As previously mentioned, mobile apps leak⁴⁰ locations, names, gender, phone numbers, and email addresses.

An App Usage report submitted by one participant showed the phone accessing 74 different apps during the 2-week tracking period, including video games like Pocket Camp and Fire Emblem Heroes; multiple social media platforms like Twitter, Facebook, Snapchat, and Instagram; and streaming services such as YouTube, Roku and Spotify. This same study participant used the Twitch app—a platform for watching livestreamed video games—for 53 hours. Twitch requires broad permissions, very similar to YouTube. Another person played Slotomania for 64 hours over the 2-week tracking period. This game requests permission to access contacts, identity, device ID and call information, media files and about 15 other items.

With the exception of two study participants who submitted data, each used Chrome to browse the web (for as many as 13 hours over a 2-week period). In addition to all the permissions listed in the above table, Google Chrome mobile browser also reads users’ “Web bookmarks and history.” The two participants who did not use the Chrome browser searched the web through the Samsung Internet app that comes pre-installed on Samsung phones. This browser requests permissions for access to a phone’s “device and app history,” “contacts,” “phone status and identity,” “location,” an array of media files, camera, microphone and much more. It cannot be uninstalled.

In addition to Chrome, usage logs showed that every participants’ phones accessed numerous Google platforms daily. These include Gmail, Calendar, Maps, Translate, Google’s search engine, the Play Store and Drive. While study participants’ devices typically accessed mobile apps for about six hours per day, the App Usage reports showed phone usage spiking as high as 22 hours on some days (see charts on next page).

40 Apps leak data to a wide range of third parties, including device manufacturers, app developers, wireless carriers, hackers and advertisers.

Date	Usage Time
3/26/19	6:59:53
3/25/19	6:10:14
3/24/19	6:16:14
3/23/19	9:16:48
3/22/19	22:23:34
3/21/19	10:13:31
3/20/19	4:44:23
3/19/19	9:46:06
Usage history, March 26, 2019-March 19, 2019	
Created by App Usage on Wednesday, March 27, 2019, 11:29 AM	

Date	Usage Time
4/7/19	14:50:44
4/6/19	11:03:36
4/5/19	7:35:20
4/4/19	9:21:36
4/3/19	7:44:23
4/2/19	6:37:40
4/1/19	22:04:04
3/31/19	16:04:50
3/30/19	13:09:39
3/29/19	17:09:29
3/28/19	8:45:49
3/27/19	10:57:21
3/26/19	8:56:29
3/25/19	11:01:06
3/24/19	4:07:24
Usage history, April 7, 2019-March 24, 2019	
Created by App Usage on Monday, April 8, 2019, 9:52 AM	

Thirteen of 14 study participants used Facebook on their phones, with participants spending as many as 23.5 hours on the app during the 2-week tracking period, according to their App Usage reports. The Facebook app for Android requests 45 unique permissions, including “read your text messages,” “read your call log,” and “download files without notification.” Instagram requests access to similar phone information.

A majority of study participants did not use native apps for retailers. However, four people installed multiple shopping apps on their phones, including: 7-Eleven,

Target, CVS, Walmart, Old Navy, Macy's, Chick-fil-A, Wetzel's Pretzels, Sephora, Footlocker, Herbalife, Forever 21, Nordstrom and Family Dollar. Mobile apps enable retailers to collect data that provide insight into each customer and to deliver “personalized, hyper-relevant experiences.”⁴¹ When customers use mobile apps, retailers gain incredible analytics capabilities—based on users’ locations, interests and online behavior—providing them with deep insights about customers. Retailers capitalize on this information to make data-driven business decisions. Because smartphone owners always carry their devices with them, mobile apps offer “a huge opportunity for hyper-targeted marketing and a level of customer engagement that can't be matched on any other channel,” according to app developer Clearbridge Mobile.⁴² The other major advantage of mobile apps is that you are given “real estate”⁴³ on your customers’ devices, which shoppers carry everywhere and always.

During a focus group discussion in Philadelphia, León said he believes it's necessary to accept cookies and grant app permissions “because that's the way things work...Hackers can find your info no matter what you do to try to protect it. Because we use the phone rather than the computer, we use the same password for everything, so we are less secure anyway.” He, like many of the participants, did not use anti-malware protection on his phone or worry about installing apps that require permission to access phone data. One participant acknowledged that “hacking and privacy breaches are bad” but, unless people personally experience these violations, “they just go out of your head.” Some claimed not to worry about privacy at all because they don't have anything “sensitive” on phones, demonstrating a lack of cognizance about how data are leaked.

During focus group discussions, community members said they observed various effects of corporate surveillance. One participant noticed that since she began working at Arby's restaurant, ads related to Arby's started appearing on websites when browsing on her phone. Another participant noted that, after sharing

41 Kosir, D. (2015, August 13). Mobile apps v. mobile web: What retailers need to know. <https://clearbridgemobile.com/mobile-apps-vs-mobile-web-what-retailers-need-to-know/>

42 *Ibid.*

43 eMarketer (2019, April 15). Retail apps gain real estate on shoppers' smartphones. <https://www.emarketer.com/content/retail-apps-gain-real-estate-on-shoppers-smartphones>

details about eating avocado toast on social media, ads related to avocado toast appeared on her phone. Other participants claimed to refuse to download apps that required “too many invasive permissions,” and one participant turned off permissions for apps that she wanted to use but considered intrusive.




We also found that, when presented with alternatives to highly-invasive Google platforms—including Gmail, the Chrome browser and Google’s search engine—study participants typically acknowledged their discomfort with a single company “knowing” so much about their online behavior. At the same time, however, very few participants said they would abandon Google products for the more secure alternative search engines DuckDuckGo and StartPage; encrypted email services such as Proton Mail and Tutanota that do not allow third parties to access emails; or the Tor browser, which allows users to anonymously browse the internet. Even study participants who were aware that Google’s business model is predicated on corporate surveillance said they were unlikely to abandon the convenience of the Google ecosystem, which extends to the calendars and translation apps on their phones. A Hispanic woman who lives in Long Beach reported that she is bothered by the fact Google uses her personal information to create a detailed profile and targeted ads. “But it would be really

hard to make the transition,” she said.

Still, a few participants were eager to test privacy-protective search engines such as Duck Duck Go or Startpage, in what might have been a modest attempt at regaining some type of control over their own feelings of powerlessness. At the same time, most participants expressed doubt that those search engines—despite assurances from the researchers—do not actually store, collect, and sell users’ information. They wanted to “stick with Google” because they know it. John rationalized his decision to continue using Google’s search engine. “In the real world we don’t really think about it. It’s the society we live in,” he said.

Because mobile technology enables continuous connectivity with family, friends and other contacts, previous scholarship has posited mobile phones as ideal for maintaining social capital. But for cell-mostly internet users, social capital may diminish as users recognize the need for phones in contemporary life. In fact, our study participants frequently said they felt discouraged about their inability to control how their mobile data are used. At a basic level, social capital emerges from the routine interactions among and between individuals

Table D. We showed focus group participants this visual prompt and asked: “Would you be willing to switch from searching the internet with Google to a more secure search platform, such as DuckDuckGo or Startpage? Why or why not?”

	<p>Name: Google Downloads: 1 billion+ Rating: 4.4/5.0</p>	<ul style="list-style-type: none"> ▪ Adjusts future search results to be based on your search history. ▪ Personalizes your feed and notifications. ▪ Google will automatically optimize results to improve loading.
	<p>Name: DuckDuckGo Downloads: 1 million+ Rating: 4.4/5.0</p>	<ul style="list-style-type: none"> ▪ Can connect without phone #, entral servers, or personal data. ▪ Searches anonymously; does not collect or share personal data. ▪ Open-source <ul style="list-style-type: none"> ▪ Anyone can contribute to DuckDuckGo’s development. ▪ Source code can be examined. ▪ Featured stories can be customized to the user’s liking.
	<p>Name: startPage Searches: 6 million+ daily searches</p>	<ul style="list-style-type: none"> ▪ Search anonymously ▪ Does not collect or share personal information ▪ Anonymous browsing ▪ Uses a proxy, not a VPN

* Data obtained from the Google Playstore and/or iTunes (2018)

and groups^{44,45} and provides an understanding of how individuals can maximize opportunities for themselves within society. The concept incorporates social trust, community and mutual benefits.⁴⁶ It suggests that when people possess abundant social connections, more resources are available to them—making it easier to take action that benefits oneself and others.⁴⁷ Bourdieu⁴⁸ takes a stark view of social capital, using it to illustrate social inequality and class stratification. He describes a system in which advantageous relationships are inherited and reproduced, assuring the continued dominance of well-connected classes. Coleman,⁴⁹ however, articulates social capital as a counterbalance to the individualistic nature of traditional economics. Coleman acknowledges that social capital can amplify privilege. But, at the same time, he frames social capital as a community resource, especially for disadvantaged groups and those whose voices are historically ignored. The wide-ranging nature of perspectives on social capital inform our research, in that our study participants express powerlessness in manifold aspects of their lives. This research seeks to obviate that powerlessness by contributing to privacy protection dialogues and policy. Moreover, Bourdieu's⁵⁰ conceptualization of the habitus describes how study participants may not be able to challenge threats to social capital, particularly as they concern data/identity protection. For Bourdieu, social capital is contingent on the context of social environment; the habitus is a world view of sorts. It describes not only a system of social practices but also an internal perception of those practices. The habitus is an internalized mode

of decision-making that individuals use based on their specific circumstances. An individual's previous thoughts and experiences—combined with personal conditions such as identity, culture, perspective, lifestyle, gender, or race—produce certain practices (habitus) in relation to action in the world (social capital). For our participants, if they receive messages from social networks saying that the price they pay for using cell phones to access vital services is to relinquish control of personal data privacy, they may accept this “fact” and not seek measures of data protection. Ultimately, class inequities are reproduced through the use of cell phones to access the internet.

We also argue that relying on mobile devices to access the internet may diminish social capital as a form of privilege. The relationships that evolve between mobile phone users and their data are “complex and reflexive.”⁵¹ Mobile phone users often have no choice but to divulge personal data, which occurs via routine actions like visiting websites, sending email and shopping online. It is impossible to control how data is monitored, stored, and shared once provided. Personal data disclosed for a specific purpose—e.g., downloading music or messaging friends—may be used for entirely different purposes by actors ranging from prospective employers to law enforcement. This leads us to conclude that, as these privacy violations accumulate, social capital as a benefit weakens. According to some study participants, the exposure of their personal data causes emotional distress about the potential for increased risk of identity theft, fraud and even safety risks.⁵² Dealing with any of these harms negatively impacts social capital, but it is especially true for people already combatting prejudice and stereotypes—the exact population most likely to rely on mobile phones for internet access. In addition, privacy violations possess potential to damage one's reputation. For example, even seemingly innocuous social media posts or web searches can later be unearthed from a database, posing a clear threat to any accrued social capital. For example, Cathy O'Neil⁵³ describes how bits of personal data from searches, posts, credit scores,

44 Uslaner, E. (2001). Volunteering and social capital: How trust and religion shape civic participation in the United States, in (Ed. E. Uslaner) *Social Capital and Participation in Everyday Life*, pp. 104-117. London: Routledge.

45 Ellison, N., Vitak, J., Steinfield, C., Gray, R. & Lampe, C. (2011). Negotiating privacy concerns and social capital needs in a social media environment. In (eds.) S. Trepte S and L. Reinecke) *Privacy Online*, pp. 19-32. Berlin: Springer.

46 Putnam, R. (2000). *Bowling alone: The collapse and revival of American community*. New York: Simon and Schuster.

47 Lin, N. (2001). *Social capital: A theory of social structure and action*. New York: Cambridge University Press.

48 Bourdieu, P. & Wacquant, L. (1992). *An invitation to reflexive sociology*. Chicago: University of Chicago Press.

49 Coleman, J. (1988). Social capital in the creation of human capital. *American Journal of Sociology* (94), S. 95-S. 120.

50 Bourdieu, P. (1990). *In other words: Essays towards a reflexive sociology*. Cambridge: Polity Press. Trans Matthew Adamson.

51 Green, L. (2002). *Communication, technology & society*. London: Sage Publications, p. 79.

52 Solove, D.J. (2007). 'I've got nothing to hide' and other misunderstandings of privacy, *San Diego Law Review*, 44, 745-72.

53 O'Neil, Cathy. (2016). *Weapons of math destruction: How big data increases inequality and threatens democracy*. New York: Crown.

or ancestry databases are used by the proprietary algorithms of insurers to generate ratings for individuals that assess risk and adjust premium prices accordingly. She argues, “in neighborhoods with more payday loan offices than insurance brokers, it’s harder to shop for

lower rates,” (p. 165) among insurers. Our participants revealed an understanding that this is happening to them. One commented, “Every time...I do something [that] involves me putting a debit card number in, or my social in...before I even do it, I ponder on it, I think about it, like, do I really want to do this?”

Trust

These potential threats to social capital are reflected in participants’ trust concerns about their phone privacy. Several participants, including León, expressed feeling as though websites and companies track their online activities. The evidence presented includes:

- “Amazon is tracking because it always sends reminders for things you might like.”
- “OfferUp calls me, then my phone warns me that it may be spam calling.”
- “I’ve started thinking, if this is going to be looked at, what will people think? I know that once I hit enter, it has the potential for other people to look at it.”
- “There is nothing that’s going to stop corporations or [businesses] from getting to your phone. You can slow down their progress, and you can do things that turn them to another avenue ... but all those lead back to your phone. It’s not going to stop.”
- Sites “are tracking your visits when you look into products, and ads tied to those specific products show up on other sites like Instagram.”
- “Low income people are victimized by platforms that are looking at and collecting our data. We are profiled through searches, etc. Is it exploitative because platforms are using ‘us’ to make discretionary decisions.

The focus group discussions revealed that some community members are conscious of phishing scams online and realize the risks associated with opening links sent from unknown sources. But others considered ad tracking to be a minor inconvenience: “It’s bothersome; I just exit when I get the ad,” one participant said. Most were unaware of the process of how this happens—through cookies, IP address, phone number, contacts, credit card information and the like. These digital traces function to slice populations into “marketable segments,”

but Shawn argues, “I don’t care if they’re doing it. I can’t stop it. I got no money to steal, and if it happens, I’ll deal with it.” Even then, some like the convenience of being able to return to favorite places online. Ivan has a home internet connection but shares a computer and primarily accesses the internet from his phone. He argued that, because he only views sports or cooking videos when on public wifi and conducts all credit card transactions on his home network, he has “nothing to hide.”

What these study participants may not realize is that retailers, cell phone carriers, social media platforms and data brokers collect, retain and analyze consumer data to obtain insights into emerging trends and preferences, and to personalize ads and marketing offers.⁵⁴ However, both purposefully and unintentionally, marketers and data brokers use their data in discriminatory ways. For example, when data brokers place consumers into “buckets”⁵⁵ that detail financial characteristics, the data may be sold to predatory businesses such as payday lenders that exploit vulnerable consumers. Similarly, marketers capitalize on consumers’ data to create differential pricing schemes or make assumptions about products and services to offer. Health insurers now collect members’ social media posts and track what they order online to “predict” how much a member’s healthcare could cost the company.⁵⁶ Real estate websites provide listings based on the searcher’s

54 Federal Trade Commission (2016, January). *Big data: A tool for inclusion or exclusion?* <https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf>.

55 Sridharan, S. (2014). Protect and survive (p. 42). *InterMEDIA* 42(3), 42-44

56 Allen, M. (2018, July 17). Health insurers are vacuuming up details about you—and it could raise your rates. *ProPublica*. <https://www.propublica.org/article/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates>

race or current zip code.⁵⁷ Payday lenders target low-income individuals. Online employment marketplaces use artificial intelligence to match job seekers with employers, but biased algorithms perpetuate inequities.⁵⁸

When prompted to consider which institutions are collecting and using their phone data, respondents indicated that corporate actors as well as the government harvest their information.

- The government collects information for “control” and to see “what’s going on with the masses.”
- “Corporations are already consolidated; they will rule the world.”
- “Government and corporations are the same thing ... corporations control the government.”
- “It’s not like I’m in corporate business, so with my phone I just brush it off. If you aren’t careful, the security systems could actually harm you ... like the government might monitor you for drug activity or something if you download anti-malware.”

These participants’ lack of trust is compounded by the discrimination that occurs through both intentional and unintentional data collection practices—as well as through both accurate and inaccurate inferences derived through their data. The dominant tech companies (Facebook, Amazon, Apple, Google, Microsoft) and providers like Verizon or AT&T use their troves of personal data to direct our online activities.⁵⁹ For instance, Facebook’s algorithms likely skewed 2016 election results by manipulating public opinion.⁶⁰ Tech company profits

are inextricably linked to governmental policies through their extensive lobbying efforts. These companies lobby, ultimately, to shape American democracy in their favor on behalf of regulatory policy, tax policy, and laws on mergers. This is true power in a governmental system beholden to the most profitable corporations. And their algorithms are trade secrets.⁶¹ Civil rights activists and technologists have raised public awareness of the unintentional algorithmic biases that influence society in significant ways—how government agencies distribute services, or how they mete out prison sentences.⁶² Such algorithmic discrimination was noted in a 2014 White House report on big data: “Big data analytics have the potential to eclipse longstanding civil rights protections in how personal data is used in housing, credit, employment, health, education, and the marketplace. Americans’ relationship with data should expand, not diminish, their opportunities and potential.”⁶³

The trust concerns exhibited by our study participants indicate that the digital exclusion of people of color and low-income Americans—which forces them to rely on smartphones to go online—does indeed limit their opportunities and potential. The findings draw attention to the discriminatory impacts (i.e. differential pricing, identity theft, customer recommendations, selective real estate listings) of mobile phone privacy infringements, analogous to existing dialogues surrounding algorithmic bias and digital exclusion.

57 Dittman Tracey, M. (2018, Nov. 2). Housing discrimination via algorithms: An alarming trend. *Realtor Magazine*. <https://magazine.realtor/daily-news/2018/11/02/housing-discrimination-via-algorithms-an-alarming-trend>

58 Bogen, M. (2019, May 6). All the ways hiring algorithms can introduce bias. *Harvard Business Review*. <https://hbr.org/2019/05/all-the-ways-hiring-algorithms-can-introduce-bias>

59 O’Neil, Cathy. (2016). *Weapons of math destruction: How big data increases inequality and threatens democracy*. New York: Crown.

60 Howard, P., Woolley, S. & Calo, R. (2018) Algorithms, bots, and political communication in the U.S. 2016 election: The challenge of automated political communication for election law and administration. *Journal of Information Technology and Politics*.

61 *Ibid.*

62 *Ibid.*

63 U.S. Executive Office of the President. (2014, May 1). *Big data: Seizing opportunities, preserving values*. <https://perma.cc/6VMK-3UJQ>

Recommendations for cell-mostly internet users:

Given the political gridlock in Washington, compounded by tech companies' massive lobbying efforts to stave off meaningful federal legislation, **we recommend these steps be taken by cell-mostly internet users themselves:**

- Activate privacy controls built into mobile devices. For example, clear your ad ID to prevent apps from tracking you, and from working with advertising network partners to track you. (Learn how to take these steps, and more, at Restore Privacy). This is effective because, while apps do not support cookies, the ad ID supplied by the operating system does. Apple makes it possible to wipe out your ad ID, and Android phones allow you to reset it.
- When apps ask for permissions irrelevant to the functionality of the app (i.e., access to your media, camera or microphone), deny these permissions. Similarly, turn off location tracking when except when needed for navigation, etc.
- Enable the "do-not-track" setting on your internet browser. It is true that only a fraction of companies respect it, some have committed to implementing it (including Pinterest and Reddit).
- Choose an email service that encrypts the messages you send and receive. And by consciously choosing websites and online services that use encryption, companies and data brokers will have far less information about your online activities.

Regulatory responsibilities

Study participants' views on who is responsible for data protection varied somewhat, but nearly all claimed that individual users were responsible for protecting themselves. For instance, focus group participants frequently pointed out that they "choose" to either skim terms of service agreements, or skip reading them altogether, before mindlessly clicking agree. "I don't read a terms of service agreement word-for-word; it's like a short book," remarked a participant in Philadelphia. Another interviewee concurred that the decision to agree with a website's privacy policy is "up to you." This cell-mostly internet user said, "If you just scroll through and hit 'I accept,' then you agreed [to the conditions]." The attitude expressed by these study participants fails to acknowledge that so-called privacy policies do not, in fact, protect users' privacy. Rather, these blanket agreements exist for companies to shield themselves from liability. It is in a company's best interest to throw in as many clauses as possible, in anticipation of nearly any potential legal scenario. One analysis found that web users would need to take a month off work annually to read all the privacy policies that pop up on their screens.⁶⁴ Online platforms offer infinite space to effectively bury language to which

users might object, were they to actually read the fine print. The attitudes expressed by our study participants do not reflect these realities. Instead, they assign blame to users who possess minimal control over how their data is mined and used. Overtly, these cell-mostly users "agree" to the terms presented. Yet they are not afforded an opportunity to challenge structural issues shaping those agreements—from the highly-invasive deals between web platforms and data brokers, to cookies that automatically leave digital "crumbs" on each website visited. "Products follow you," one participant stated, with no mention of how this surveillance is able to occur. This study finding symbolizes a type of acquiescent self-reliance.

Nevertheless, the responses indicate mixed views about the nature of regulatory responsibility and about the extent to which protections are already in place. Many participants supported a "law that protects your data," but their concerns about privacy violations were not sufficient to outweigh desires to use their favorite apps. One participant claimed that "terms of service" constitute "laws" that protect mobile phone users. Another participant stated, "If I'm not doing anything wrong, so what?" Most don't read privacy policies or terms of service agreements because they are "taxing to read," long, and redundant. One person argued that, whether or not our data are protected, websites and apps collect too much data on individuals.

64 McDonald, A. & Cranor, L. (2008). The cost of reading privacy policies. *I/S: A Journal of Law and Policy for the Information Society*, 4, 540-565.

These statements were provided in response to questions about responsibilities for data privacy:

- “We should be responsible for ourselves, but we don’t have any privacy anyway because if you want to apply for a job, you HAVE to go online. So you’re already giving up your data!”
- “It is our own privacy, so we should have full ownership and responsibility for it.”
- “It is the user’s choice to subscribe to its features, and their responsibility to protect their own data.”
- “Privacy policies exist supposedly to cover you.”
- “We have to be more aware, but we shouldn’t have to do that. There should be a security tutorial for phones.”
- “We should be responsible, but also the government ... Companies that collect our data should hold some responsibility towards protecting it.”

When prompted to explain further, a number of focus group attendees argued that the companies that create the services (e.g., app developers, ISPs, platforms, phone manufacturers and carriers) should be able to create their own policies. However, many hoped the government would create ethics guidelines to which all companies must adhere once “more people understand how the internet works.” But many thought such guidelines were weak. Kyle, an iPhone user, suggested that phone manufacturers as well as service providers like T-Mobile share a dual responsibility to educate users about data protection at the point of purchase. “Like Apple Care, with extra security options available through the carrier ... the user feels at ease when you know that you got two walls of protection.” Kyle added, “it should be illegal” to buy and sell personal information, asserting that data brokers “prey on the ignorant.” Two participants argued that the president should be responsible for phone data protection, while many others suggested that Congress or state leaders should implement some type of legal regime for data protection. A few suggested that we, the researchers, create phone privacy workshops for them, which they’d “gladly attend” as what participant Dolores termed “a movement toward being more tech savvy for civilians.”

Despite the variety of suggestions regarding data security accountability, many were pessimistic that

any regulations or tutorials would be implemented, as indicated in these responses:

- “Never going to happen...because of terrorism.”
- “It’s all about profit. That’s what it comes down to. If it’s not about the safety of this country. It’s about how much, you know, profit [they] can make ... no way.”
- “The corporations and government...don’t want us to know. People would then find ways to manipulate information for [power].”
- “Government will not create laws that give online users the “rights” to their information. They will not get anything out of it. They want all of the profit.”
- “We accept it.”
- “My mind just goes more to my kind of people. The people who can’t afford a lawyer to go and fight. The cops won’t care about us if something bad happens because our information was stolen by somebody in Ohio, Nebraska, or Russia, or Guam. I know I’m sitting in a room with a bunch of people who don’t have that influence and probably never will. If we don’t help ourselves, who the hell will?”

These responses signal a perceived lack of agency not only over personal data but also in society. Participants who claim that individual users rather than the government or companies or developers should take responsibility for privacy are acceding to the discourse of privacy as an individual choice rather than a social good (or as a basic human right). There is little understanding of the many facets of the surveillance economy in which they participate. But the surveillance economy objectifies individuals, reducing them to data points. Conceptualizing data privacy as a social good requires that it is unavailable to be traded for convenience or efficiency or even security.⁶⁵ For cell-mostly internet users, who are economically disadvantaged, the surveillance economy places them in precarious spaces where they’re vulnerable to identity theft, fraud, predatory scams, and unequal evaluation of credit worthiness or even immigration status. These vulnerabilities are the essence of digital inequality and lack of social capital.

⁶⁵ Steeves, Valerie M. (2009). Reclaiming the social value of privacy. In Lucock, Carole, Steeves, Valerie M., Kerr, Ian. (Eds), pp. 191-208. *Lessons From the Identity Trail : Anonymity, Privacy and Identity in a Networked Society*. New York: Oxford University Press.

Recommendations for policymakers

In the past year alone, consumers have learned about privacy scandals from some of the country's largest technology companies. We found out that Cambridge Analytica harvested the personal data associated with millions of Facebook profiles without consent, and used it for political purposes. The technology site Motherboard exposed that major wireless carriers sell real-time data to bounty hunters for a \$300 fee. We learned that Google+ bugs provided third-party app developers access to millions of users' personal information, and that an Amazon Echo inadvertently shared a recording of a couple's private conversation. For every high-profile case, there are many more that do not get attention in the press and that the FTC does not address. Nevertheless, consumers experience harm from lesser-known privacy and data security incidents.

- For this reason, we recommend that Congress increase FTC funding by at least \$40 million annually (beyond its current budget request of \$310 million) to hire technologists who can develop cases and make policy recommendations, as well as hire dozens of new attorneys focused on privacy and data security. We believe such a funding boost

would provide the FTC with the resources to hold technology companies, retailers and data brokers accountable for their data practices.

- Bar social media companies from purchasing/selling personal information to data brokers and advertisers without an explicit "opt in" from users.
- Empower the FTC to take immediate enforcement action against tech companies and data brokers that track, store and share personal information without user consent.
- Regulate data brokers to require transparency in data gathering and manipulation techniques.

In the absence of nationwide data privacy legislation, the federal government should:

- Fund a series of data privacy workshops administered by non-profits in distressed urban areas.
- Allow states to adopt stringent data privacy measures that supersede weaker federal regulations.

Willingness to act

Because participants nearly always associated privacy breaches with the government rather than corporations, online advertising agencies or social media platforms, most were unwilling to pay for extra phone security because "the government already has your information." One participant would not pay because "there's another third party that might try to steal your info; hackers will always find a way." Another participant asserted, "I see no benefit." León purchased a security program, but he wasn't sure if it actually helped. But some said they were willing to pay under particular conditions.

- "I would pay if the protection charge is something reasonable."
- "At least, if you pay, you can complain to someone if anything or even nothing happens. If you go to a store and get a guarantee or warranty, you can complain.

But there isn't such a thing with these apps."

- "Not everyone can pay for security ... if you have a family of 3-4, the protection costs too much."
- "Once you add up the taxes, it's just too much. But if it was \$10 a year ..."
- "Yeah, \$10 a year is my price range."
- "That's affordable; it could be a standard charge when you buy your phone."
- "I would pay \$40 a year but not \$100."
- "A security fee should be included in the monthly phone bill."
- "There could be a sliding scale price range—pay more for better security."
- "I would pay not to get scam offers."

- “I am willing to pay \$2-\$5 a month, depending on what it is actually going to protect. I’m real paranoid about giving out personal information.”

Besides working to protect their own data—to an extent—no participants expressed willingness to act

in other ways to protect themselves from some of the harms associated with data leakage and the surveillance economy. This finding indicates that cell-mostly internet users do not prioritize the types of actions, such as installing anti-virus software or a firewall, that could mitigate at least a few mobile phone privacy harms.

Recommendations for tech companies, mobile phone carriers, and consumer privacy advocates

Based on findings from focus group discussions and app usage data, **we propose the following recommendations for technology companies and mobile phone carriers:**

- Obtain opt-in consent from consumers and subscribers before sharing sensitive information about them.
- Explain to users the importance of installing updates and security patches.
- Develop free anti-malware shareware for qualifying low-income users and pre-install it on phones.
- Create tutorial videos that can be accessed in-store and online that spell out processes for securing phones. Train sales personnel to help consumers implement the video suggestions. Videos can be funded through a \$1 surcharge on all new phones sold in the United States.

These recommendations lead us to conclude advocacy groups have the potential to influence tech platforms, regulators and users. **With this in mind, we offer the following recommendations for consumer privacy advocates:**

- Make data privacy a political issue—on par with health care and minimum wage legislation—and force legislators to act. Adopt the stance that data privacy is a fundamental human right.
- Pressure social media sites and companies to reform their data collection practices. Specifically, press to obtain consent from customers before using or sharing their personal information, and give consumers the right to know how their personal data are being used. Businesses also have an obligation to provide consumers with a copy of any personal information they possess.
- Demand that companies notify consumers of a security breach within 72 hours.
- Work with consumers to create a public education campaign to frame mobile phone privacy as a basic right and a social justice issue to empower users on methods to secure their data.

Conclusion

In general, the cell-mostly internet users interviewed for this project recognize the existence of corporate and government surveillance. As our findings highlight, some of them even compromise personal relationships or relinquish job opportunities, rather than share personal details on social media or to complete online forms. At the same time, participants lacked a clear understanding of how near-constant mobile internet use, including dependence on internet-connected apps, potentially compounds other inequalities that exist in their lives. Rather, study participants generally seemed resigned to their status as having little power and minimal social capital. All individuals are vulnerable to security breaches, identity fraud, system errors and hacking. But economically disadvantaged individuals who rely exclusively on their mobile phones to access the internet are disproportionately exploited through leakier phone models, lack of knowledge about phone security practices, and attitudes of resignation with regard to their agency over their own data. Such users are also more open to governmental surveillance if they participate in programs for low-income individuals and families such as SNAP (Supplemental Nutrition Assistance Program) or live in subsidized housing. Moreover, trust in governmental organizations may be shattered when data collected for public programs are used in problematic ways by agencies that lack transparency.

Throughout this paper, we argue that privacy is a public good and a fundamental value in a democratic society. In fact, it is a requirement of basic human dignity.

Because of the sheer ubiquity of digitized data compiled on individuals who rely on cell phones to access the internet, we argue that the need for privacy be elevated from a personal liberty and legal right to a matter of social justice. Data privacy is not a luxury for those who cannot afford to invest the time, resources, and effort required to actively protect one's digital assets.

Our project findings shine light on an increasingly serious problem of digital life—the inequities exacerbated by data insecurity that are experienced by all individuals but are more salient among those living in economic precarity. Also, the project is vital to advancing STS by building on the field's emerging activist strains. When Google and other technology companies capitalize on the data exhaust left by cell mostly internet users by using it for creating predictive analytics—without transparency of methods—the inequities experienced by these users are only compounded.

With the EU General Data Protection Regulation now in effect, albeit slowly and incompletely,⁶⁶ these study findings underscore the need for U.S. citizens, lawmakers, and activists to further consider the grassroots impact of data privacy and security. Additionally, we hope this research will empower cell-mostly internet users—who are likely black, Hispanic and/or low-income—by bolstering digital literacy around mobile technology privacy and security. Understanding the symbiotic relationship between the material nature of mobile technology and the social construction of technology is a key means to safeguarding privacy in our increasingly digital lives.

66 Scott, M., Cerulus, L. & Overly, S. (2019, May 29). How Silicon Valley gamed Europe's privacy rules. Retrieved from <https://www.politico.eu/article/europe-data-protection-gdpr-general-data-protection-regulation-facebook-google/>

Appendix A. Semi-structured interview protocol for focus group discussions

How would you describe your attitudes about online privacy and security in general? How about with regard to your mobile phone, specifically?

Do you use a pre-paid or burner phone? If so, how does this influence how you use the device?

Do you use an Android or iPhone mobile device? Did security concerns influence your decision?

Do you delete “cookies” on your phone? Do you know how to do it? To what extent are you concerned about cookies on your phone?

Do you empty your cache on your phone? Do you know how to do it? To what extent are you concerned about your phone’s cache?

Who determines what data websites and apps may collect about users? Even if you don’t know for certain, who do you guess sets the rules for data collection?

Would you use security features on your phone if they were available? How much, if anything, would you be willing to pay for mobile phone security measures?



To what extent should government, tech companies, or businesses be responsible for ensuring consumer privacy?

Have you or anyone you know had issues with mobile phone security (e.g., identity theft or hacking)?

Vignette A: Verizon introduced a mobile app called AppFlash, which acts as a search engine for users looking for everything from restaurants to music. But its primary function is to collect data from the customer’s mobile number, the device he/she is using and the apps installed. With users’ permission, it will also monitor location and contacts. Would you be willing to use AppFlash, if it is more accurate and faster than Google or another search engine?

Vignette B: Facebook’s Live Location feature makes it possible to share your location in real time, with a single person or groups. The selected people can track your location for 1 hour. So, suppose if you are meeting friends for a concert and you are running late, this feature will allow your friends to know how much time you will take to reach the place. Would it bother you if Facebook sold this geo-location data to 3rd parties? Would you be concerned that a hacker might learn you are away from home?

Appendix B. Example visual prompts

	<p>Name: Facebook Messenger Downloads: 1 billion+ Rating: 4.0/5.0</p>	<ul style="list-style-type: none"> • Turn location on to let people know you're nearby • Free calls over Wi-Fi • Active while not in use
	<p>Name: ChatSecure Downloads: 500,000 Rating: 4.3/5.0</p>	<ul style="list-style-type: none"> • Can connect without phone #, central servers, or personal data • Uses known open source cryptographic libraries to maintain privacy • Can connect to existing accounts on Google, create new accounts on public XMPP servers, or connect to secure server

Appendix C. Example of cyclical, iterative, and rigorous coding method using Nvivo 12

