

How Do You Turn a Mobile Device into a Political Tool?

Amelia Acker
School of Information
The University of Texas, Austin
aacker@ischool.utexas.edu

Brian Beaton
Center for Expressive Tech
Cal Poly (San Luis Obispo)
brbeaton@calpoly.edu

Abstract

This paper reports on findings from an ongoing study of recent software applications that attempt to turn mobile ICT's into political tools. The software in question endeavors to make new types of political behavior expressible for ICT users. Two troubling trends were found. The first involves incommensurability between backend databases and the data traces generated by users. The second involves the production of data and metadata vulnerabilities. As part of discussing these trends, the authors introduce the idea of "minor apps" and argue for their importance within discussions of sociotechnical aspects of digital infrastructure.

1. Introduction

This paper shares findings from a recent study of software applications that were principally designed for use on mobile ICTs: information and communication technologies scaled for portability, such as smartphones and tablets that run mobile operating systems like Android, BlackBerry OS, iOS, Nokia X or Tizen. Mobile ICTs support factory-installed or user-downloaded "apps" (i.e., software applications) that leverage the device's size, location, hardware functions (e.g., camera, audio, memory), and commercial wireless networks to enable new forms of human communication, public sociality, engagement with space and place, and new forms of being in the world (immersed, augmented). Such devices and the software that runs on them, as we highlight in this paper, have also begun to enable new forms of political behavior that have little resemblance to the famous cases of Occupy Wall Street and Arab Spring [7], which played such a key role in demonstrating the political potential of ICTs but as historical events are increasingly distant from the digital and data infrastructures of our current moment.

Mobile ICTs are spreading (i.e., achieving technological saturation) and diversifying at a rate previously unwitnessed in human history. No other documented technology of which we know has moved so quickly into so many hands and cultures, but also taken such a variety of slightly different forms and capabilities while doing so. By the end of 2015, there were reported to be over 7 billion mobile cellular subscriptions in the world. In addition, the International Telecommunications Union estimates that there will be approximately 6.1 billion smartphones in the world by 2020, which is also when we expect to see 5th generation (5G) mobile networks in place, whose creators are promising faster data transmission rates, increased coverage, and more [11].

How mobile subscriptions are counted is a topic of ongoing controversy because what actually gets counted in such reports are SIM connections and not unique human subscribers. Similarly, what counts as a smartphone is not typically well-defined in estimates of smartphones. Nonetheless, it has become incontrovertible that mobile ICTs and their "apps" are now a key part of our digital and data infrastructures, not only here in Hawaii but also globally [11]. The published numbers, although not wholly accurate, are themselves further proof: how mobile ICTs are not yet countable in precise and sophisticated ways is a testament to the pace of their creation, spread, and permutation.

Because of these developments, studies of mobile ICTs and the software created for them can follow a number of different research paths. Our research concentrates on recent efforts to develop apps that allow people to express their political views in new ways or that allow people to engage in political struggle in ways that were not previously doable, perhaps even as recently as 2010 or 2012. We study efforts to turn current-generation mobile devices into political tools, and we try to keep our attention focused on the very latest happenings in this domain. In doing so, we track new mobile hardware and software as it gets developed and released, study the

social impact of mobile technologies, and study the ways in which existing patterns of human culture and behavior inform the creation and use of mobile ICTs. Within this broader research agenda, we maintain a particular focus on new and emerging enactments of political behavior that directly involve the operationalization of mobile devices like smartphones and tablets.

All mobile devices are “political tools” to some degree, one could argue. For example, such devices are typically bound up with controversial processes of natural resource extraction (mining for coltan, copper, iron, nickel, tungsten, etc.); imbricated within global supply chains that mobilize alienated labor; and popularly understood only through the veneer of advertising strategies that are created by experts in fields like consumer behavior and marketing psychology [3] to purposefully shape public beliefs and sentiments [6]. Such devices are also bound up with sexed, gendered and racialized cultures of hardware and software engineering that continue to be male-dominated and majority-white, at least in the United States, which is where we focus the bulk of our research attention.

Each of these topics warrants careful study and further attention. But our research specifically focuses on how mobile devices allow users to create new political possibilities for themselves in real time: different ways of being in the world, different ways of being socially situated, and different ways of engaging with uneven distributions of resources, risk, opportunity, and power. Our larger goal is to understand how digital platforms and infrastructures are sites of political interaction today, starting with the idea that such interactions have the potential to change quickly given the current rate of technological saturation and diversification in the domain of mobile ICTs.

This research on mobile ICTs and our mobilization of the term political tools builds directly on the sizable (and still-growing) body of academic literature that explores the fascinating and multi-layered links between everyday political culture and digital media [4, 13, 18]. Our work also draws inspiration from the growing body of research that looks at the use of mobile ICTs within social movements [9, 10, 16]. These bodies of scholarship have accomplished several things that continue to be foundational to our own work: justifying mobile ICT’s as a valid object of academic study; establishing that digital and data infrastructures are increasingly entangled with political cultures; and making discussable the links between hardware, software, information systems, information services, and quotidian political behavior.

Our research adds to this exciting body of work by shifting some of the empirical attention to “minor” apps that lack large developer teams, large user communities, high levels of financing, and/or discernible plans for maintenance and sustainability. Much of the published research, at least so far, focuses on engagements with ICTs that mobilize large user communities (e.g., Twitter or Instagram) and rely upon a high path dependency on cloud computing and networked platforms for web-based databases and storage (for example, Gmail or Facebook). In these cases, the apps in question typically force the users to access data on a web-based client instead of access data on their internal storage, and further, such apps typically encourage users to let the software continuously run in the background of their mobile devices and passively collect new data such as recent pictures or one’s current location. Such major apps facilitate a captivating range of political behaviors and will almost certainly continue to do so.

We wondered, though, about the thousands of apps that are developed and published or sold that don’t aim to have millions of downloads but are only intended for tens or hundreds of downloads at best. In fact, most apps arguably fit on a matrix of at least two axes (see Figure 1.), where one axis moves from mainstream to niche user communities. The other axis concerns where data is collected and stored (i.e., what is done with data). In our research, we have begun to explore apps that aim to support or service niche user communities and on apps that encourage users to leverage the internal storage on their devices.

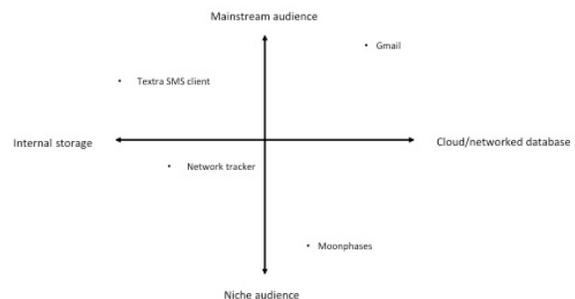


Figure 1. Matrix of users and data storage

As we’re discovering in our work, which is ongoing and exploratory, and as we discuss in further detail below, much of the software in this other quadrant (what we call “minor apps”) seems to work as little more than a rudimentary pairing of databases and data traces: the software lacks much of the functionality and ‘app-iness’ that current generation

ICT users would normatively expect with regard to features, look, and feel (user interface). However, we argue that some provocative developments are nonetheless occurring when it comes to people's political behavior and when it comes to the idea of using mobile devices as political tools.

2. Method and Design

The paper unfolds in the following manner: we begin by further elaborating on the idea of minor apps and argue for their importance as objects of study for those interested in the "complicated relationship" [14] that people have with mobile ICTs. We then detail some of our latest research findings, focusing on 6 of the apps that we've been investigating among a larger body (N=18). All 6 are English-language examples from the United States, an acknowledged limitation of our work. Another limitation: we chose to limit our discussion here to mobile apps that are available free of cost and developed for Android and iOS, two of the most popular and accessible mobile operating systems for users of smartphones and for developers designing and publishing apps [15]. Following the section on minor apps, we focus on some of the glitches and limitations that we've been discovering by analyzing the data traces generated by minor apps, how the apps utilize databases, and issues of metadata creation. We conclude the paper with a discussion of why this research matters to those concerned with the sociotechnical aspects of digital infrastructure and sketch some directions of future research.

The apps that we discuss in this paper include the following: Flyrights, an app geared toward the Sikh community that promises to document and map incidents of discrimination or profiling at airport checkpoints managed by the U.S. Transportation Security Administration (TSA); Testee, an app primarily geared toward "millennials" that allows users to share STD/STI test results in a Snapchat-like fashion, with a promise to immediately delete the records, as a way to promote sexual frankness and to disrupt cultural legacies of shaming around sex (many of which are heteronormative legacies, in addition to being anti-sex); RedLightTraffic, an app that allows users to report suspected incidents of human trafficking that works like a citizen law enforcement tool for curbing sexual slavery and contemporary articulations of sexualized slave labor; Hinder, a Tinder parody app that promises to expose anti-abortion and "anti-women" politicians and government officials; and We-Consent, an app that allows users to create a video record of one's

affirmative consent to sexual activity, just before having sex, as a way to push back on and challenge American rape cultures. Each of the 6 apps discussed in this paper is a minor app with limited functionality and a relatively small user community.

Much of our research and discussion is grounded in data trace analysis. This kind of data trace analysis represents a methodological innovation for information and communication scholars grappling with the rapid updates and near-constant terms of service (ToS) changes found in contemporary mobile ICTs and networked platforms. Much of our research and discussion also builds on methodological and empirical research trends circulated at HICSS specifically, which as a scholarly community has become one of the principal sites of methodological innovation when it comes to critically investigating digital and data infrastructures.

3. What is a minor app?

Apps are software applications that run on mobile operating systems. Apps also leverage device capabilities and access commercial wireless networks that connect users to the internet. A number of apps come pre-installed on current-generation mobile devices, but most users download them from app stores (e.g., Google Play Store and iTunes App Store), which are online marketplaces that manage and control app consumption patterns and planned obsolescence patterns by way of developer guidelines and managed distribution channels. It should also be noted: the majority of apps developed for and distributed through app stores are proprietary software. While many are "free" to users, the source code cannot usually be changed or modified by users. In earlier work, we found that such patterns of software production and consumption on the part of app stores and mobile device and app developers leads to routine software updates and, at times, software update unrest on the part of software users because developer control over apps and their versioning can significantly reorganize and upend software user experiences [2]. In other words: we had already discovered that apps could be sites of politics and political contestation, but we had not considered the idea of major and minor apps.

Part of our delay in realizing the existence of such apps (or the generativeness of such distinctions) is that apps were not always a prominent aspect of mobile ICTs. For example, first-generation mobile phones on 2G networks, also known as "feature phones," had only a few functions, such as an address book, calendar, and text message client. As mobile broadband internet coverage increased with 3G

networks, smartphones that connect to the internet have increased in production and popularity. Consequently, the app market has grown to represent a new and interesting distribution model for software. Instead of using a traditional file structure (tree-style directory format) to access individual files (like .jpeg and .mp3), contemporary smartphone operating systems rely heavily on downloaded and updateable apps that allow users to create and access networked databases, typically via cloud infrastructures. As compared to feature phones, many of the most popular and widely-used smartphone apps today are largely designed to transmit data (i.e., push data out or pull data down) and not necessarily to create or store data internally on the mobile device. Yet this change over time is marked by internal diversity: fundamental differences are emerging between apps and not all “new” apps are necessarily making use of current-generation digital and data infrastructures.

In their groundbreaking research on cultures of software development, Christopher Kelty and Seth Erickson argue: “Software is neither material nor immaterial but durable, entrenched and scaffolded” [12]. For Kelty and Erickson, moreover, the study of software is also the study of people: the existence of software “implies an ecology of users, designers, maintainers, as well as organizations and physical facilities that must be kept running and made durable”. One way, then, of approaching the “software app” as an object of study is to think about how users of mobile ICTs are always situated within a complex social milieu that operates in the “background” of any mobile device, often invisible to users yet nonetheless co-shaping what is thinkable and doable with mobile devices. One must also keep in mind the various mobile operating systems, competing app markets, and the billions of active mobile devices now connected to wireless networks which together create a polyphonic range of software apps and app experiences that mark slightly different technological moments (e.g., 2011, 2014, 2017), depending on the creation date and update history, and possess different levels of vitality (or “durability”).

In shifting our research attention to minor apps, we were initially uncertain as to how such apps might differ from or reinforce the patterns of software production and use documented by other researchers, such as Kelty and Erickson. We were also uncertain as to the criteria for calling an app minor. But several things became apparent as we began to explore this other quadrant of app development and use, and as we began to group minor apps together into what we argue is a coherent object of study, much like the “minor literature” analyzed by Gilles Deleuze and

Félix Guattari [8]. Our working definition of minor apps, which we enthusiastically invite others to trouble or revise, is that such apps are politically unambiguous; uniquely particular in their intended audience; developed by or for those who hold marginalized positions in society; cannot as applications fully capitalize on current hardware and software capabilities; and cannot as applications fully capitalize on current digital and data infrastructures. Minor apps are inelegant but radical in potential. They don’t always work as described or intended but they mark a fundamental shift in the longer history of how ICTs and political culture interoperate, something dramatically different from what other researchers found in the cases of Occupy Wall Street or Arab Spring, to offer two better known examples of ICTs intermixing with political behavior.

4. Findings: Some trends in minor apps

One of the major trends that we’re observing during our research is something that we began calling “glitchbait.” Glitchbait apps oversell what they promise to do for users. After one or two uses, glitchbait apps become meaningless because they don’t offer users updated or tailored information to their needs (“junkware” is a similar term used by others). The mismatch between most of these bait and glitch apps has to do with an incommensurability between the data traces that the user would create (presumably submit to the developers), and the time or space limits of the databases that the app queries to match the desired function.

For example, with Hinder, the profiles of anti-abortion and “anti-women” politicians and government officials are served up in a user’s matching stream, like its reference point, Tinder, the popular dating app. The profiles served up to the user are based on a user’s location. Users in, say, Santa Barbara would initially receive profile matches that detail the ideologies or viewpoints of California state representatives. But once a user has swiped through a small number of “anti-women” (a term never fully pinned down or defined) politicians and political leaders, California in this scenario, the app begins to feed profiles from nearby states without notification or without the ability to return to California profiles. The user has to swipe through a whole database of anti-abortion and “anti-women” politicians in the US before getting back to California. Admittedly, reality is always more complex than any database structure can depict [5], but the user’s GPS location information doesn’t scope out or limit the stream of possibilities based on

location limits for which the app claims to be purpose-built, as one would find in other swiping apps, such as the more well-known apps Tinder and Hinge. In the mobile dating apps that Hinder is based on (and parodying), setting location limits and targeted radiuses are major design features [17]. Because users can, by law, only vote in the state of their residence, how the Hinder app fumbles with location services, and the physical worldliness of mobile ICT's, means that it starts flooding users with potentially irrelevant data.

FlyRights is another glitchbait app. The app isn't dynamic or reflective of user uploads in real time, nor does it appear that the developers are regularly submitting incidents of airport profiling. In this case, instead of a frontend glitch with accessing the right data or database, the app has a backend glitch with the systems reporting database, which doesn't update frequently to absorb trace data from users based on their new (and ongoing) racial profiling encounters at TSA checkpoints. In the case of FlyRights, the database of incident reports is perpetually outdated and misrepresents the rate and severity of airport profiling, the very problem the app aims to empower users to help chronicle and combat.

In both of these cases, the developers seem to be struggling to resolve how to achieve each app's central promise. Ineffectively folding in new data traces makes each app produce biased or flawed results. In each of these cases the "bait" is an app that works with up-to-date trace data submitted by users, the glitch is that these apps don't succeed because the database is populated with outdated data or with poor limits on the data being accessed.

A second trend that we're observing in our research is evidence that minor apps are creating data and metadata traces that have afterlives or secondary use applications that may be unknown to users or perhaps even to the app developers themselves. Certain data traces may serve as "metadata" in one context because they provide information about people's activity or behaviors, but they may also serve as "data" if they are themselves analyzed in other contexts and used as evidence to make a claim or argument [1]. For example, the user-generated content submitted through RedlightTraffic, Testee, and We-Consent produce location data that would have been previously difficult to collect. While each app's intended purpose is to create data for storage and secure transmission privately, the app delivery receipts also appear in download caches of the devices themselves, even after they have been deleted. In each of these apps, device features are harnessed to produce technical information about the time, place, and size of any data transmission. These

technical data are background to the user, but are essential to the functioning of each app.

Often when we download and share our data with mobile apps, we "dubiously consent" (sometimes called "dubcon" in other contexts) to create metadata that will have unknown consequences in the future, perhaps even for which the developers themselves cannot speculate. Downloading the app from the Google Play Store or Apple's iTunes App store creates a record of transaction on the marketplaces as well as on the storage directory of the device's operating system. Once users download and begin to use each of these apps, there remains a history of transmission and timestamp. Dubcon apps such as these create metadata with strange afterlives: users give consent to create and transmit data, but it remains unclear whether they would consent to the powerful metadata created as part of the process if future use cases of metadata could be known. Just as the appearance of a colleague's email address in the recent Ashley Madison data dump points to particular kinds of use, the existence of Redlight Traffic, Testee, and We-Consent on your download cache points to speculative use cases of the intent and outcome of making use of these apps. Despite their up-front (seemingly clear) and functional origins, aggregated metadata or metadata taken out of context can play different roles for different stakeholders within digital and data infrastructures. These metadata can become more powerful evidence than the content initially created by the user, and in these particular cases can be used to track political activity and behavior.

5. Discussion and Conclusion

The mobile apps that we've been examining in our research represent some of the edges of digital culture and app development. They have niche user communities and limited functionality. But each seems purpose-built for engaging in expressly political behavior. Each tries to make new kinds of political behavior afforded, to use the language of affordances. Developed for mobile ICTs, the apps try to immerse technology into a user's political life in new ways, or to augment a user's engagement with and relationship to pre-existing (*and often longstanding, embodied*) political struggles around physical and cultural differences, and around the uneven distribution of resources, risk, opportunity, and power in society. The user may not have any prior relationships with or fluencies in these specific political struggles, nor the app developers. That makes the apps that we've been studying all the more fascinating: the links between what we're calling

minor apps and more famous examples of political behavior involving digital platforms and infrastructures are not immediately clear. In many ways, we hope that's one of the central contributions of this paper: shifting the empirical attention and calling attention to minor apps as political grounds.

Two major trends that we've been observing in our research, which focuses on the United States, are the following: (1) a common disconnection between the data traces and databases underpinning minor app functionality and (2) the active production of data vulnerabilities due to how minor apps create and store data and metadata traces. As our research continues, we intend to look for these trends across a greater range of minor apps, which this paper posits is a useful term or category of analysis for critically talking about sociotechnical aspects of digital infrastructure, the focus of our discussion here as we elaborate on why this research matters and articulate some directions for future research.

Our research presented here begins to shed light on several sociotechnical aspects of the worlds underpinning minor app development and surrounding minor application use. One possibility is that an alternate way of making digital and data infrastructure is starting to root into commercial app stores and, moreover, doing so despite breaking from the normative conventions that mainstream users might associate with "good" design practice or app development. If that's the case, minor apps of this type could represent a purpose-built materialization of political values, a tangible example of "appiness" denied on the part of app designers and developers who want to create some other form of user experience and engagement because they hold an alternate perspective on either digital platforms, infrastructures, or both.

A second possibility is that what we're currently reading as troubling trends are in fact manifestations of *tension* between commercial wireless providers and minor app developers, between mobile hardware makers and minor app developers, or some combination thereof (depending on the app in question, the nature of the glitches or vulnerabilities, and the particular actor groups involved). Informed by the research presented here and by ongoing discussions at HICSS, we remain open in our research to the possibility that what we're beginning to discover is actually a broader set of tensions that potentially involve not only a thick social layer but also the thick physical layer that comprises commercial "wireless" networks and "wireless" communications.

A third possibility is that fundamental skill and knowledge gaps exist among those trying to turn

mobile devices into political tools. Who gets to participate in politically experimenting with ICTs, and what they know and can do as app designers and developers, is almost certainly shaped by pre-existing patterns of privilege and opportunity. These examples may be cases of limits and limiting factors: "the best that can be done" by these particular developer communities.

As we continue to carry out work on what we think is an important and understudied topic, what we expect to find on the near horizon is not just one or two mega-platforms for political behavior but a planet populated by a litany of minor apps, for all different types of users and political contexts, and for all different types of mobile devices. In their current instantiation, such tools try to do things like give people the situational capacity to add to running, open-ended data resources designed for public use or push data about specific political causes or allow people to create new kinds of records as a way of being politically engaged or allow people to find politically-charged resources or services. But such tools have a level of particularity to them that frequent users of major apps would likely find unusual, along with a high level of "dysfunctionality" for lack of a more appropriate term.

Directions for future research include a broader investigation of "appiness" and its denial in existing app marketplaces, studies of practice that attend to tensions between the actor groups involved in the design, production and use of minor apps as well as explore if and how such tensions find materialization, and investigations of skill and knowledge inequities within app developer communities that may be limiting what's thinkable and doable with mobile ICTs among those working at the very edges of technology-assisted political behavior.

6. References

- [1] A. Acker, "Radical Appraisal Practices and the Mobile Forensic Imaginary." *Archive Journal*, 2015, 5(1).
- [2] A. Acker, B. Beaton, "Software Update Unrest: The Recent Happenings Around Tinder and Tesla", 49th Hawaii International Conference on System Sciences (HICSS), IEEE 2016, pp. 1891-1900.
- [3] J. Agar, *Constant Touch*, Icon Books, United Kingdom, 2013.
- [4] N. K. Baym, *Personal connections in the digital age*. John Wiley & Sons, New Jersey, 2015.

- [5] G. C. Bowker, "Big Data, Big Questions | The Theory/Data Thing", *International Journal of Communication*, 2014, 8(2043), pp. 1795–1799.
- [6] S. Braman, *Change of state: Information, policy, and power*, MIT Press, Cambridge, 2009.
- [7] M. Castells, *Networks of Outrage and Hope: Social Movements in the Internet Age*, Polity Press, Cambridge, UK, 2012.
- [8] G. Deleuze, F. Guattari, *Toward a Minor Literature*, University of Minnesota Press, Minneapolis, 1986.
- [9] J. Donovan, "'Can you hear me now?' Phreaking the party line from operators to occupy", *Information, Communication & Society*, 2016, 19(5): 601-17.
- [10] J. Donner, *After Access: Inclusion, Development, and a More Mobile Internet*, MIT Press, Cambridge, 2015.
- [11] International Telecommunications Union, "World Telecommunication/ICT Indicators database 2015 (19th Edition/December 2015)", ITU, Switzerland, 2015.
- [12] C. M. Kelty, and S. Erickson, "The Durability of Software," in I. Kaldrack, and M. Leeker, *There is no Software, there are only Services*, Meson Press, Lüneburg, Germany, 2015, pp. 39-56.
- [13] B. D. Loader, and D. Mercea, "Networking democracy? Social media innovations and participatory politics", *Information, Communication & Society*, 2011, 14(6), pp. 757-69.
- [14] P. D. Miller, S. Matviyenko, *The Imaginary App*, MIT Press, Cambridge, 2014.
- [15] R. M. Müller, B. Kijl, J.K. Martens, "A comparison of inter-organizational business models of mobile app stores: There is more than open vs. closed." *Journal of theoretical and applied electronic commerce research*, 2011, 6(2), pp. 63-76.
- [16] K. Thorson, K. Driscoll, B. Ekdale, S. Edgerly, L.G. Thompson, A. Schrock, L. Swartz, E.K. Vraga, C. Wells, "YouTube, Twitter and the Occupy movement: Connecting content and circulation practices", *Information, Communication & Society*, 2013, 16(3), pp. 421-51.
- [17] Tinder, "Privacy", Tinder, Inc., 2016, <https://www.gotinder.com/privacy>.
- [18] E. C. Weinstein, "The personal is political on social media: Online civic expression patterns and pathways among civically engaged youth", *International Journal of Communication*, 2014, 8, p. 24.