Linking Platforms, Practices, and Developer Ethics: Levers for Privacy Discourse in Mobile Application Development

Katie Shilton & Daniel Greene

Journal of Business Ethics

ISSN 0167-4544

J Bus Ethics
DOI 10.1007/s10551-017-3504-8

Springer

J Bus Ethics
DOI 10.1007/s10551-017-3504-8

ORIGINAL PAPER

Linking Platforms, Practices, and Developer Ethics: Levers for Privacy Discourse in Mobile Application Development

Katie Shilton[1] · **Daniel Greene**[2]

Received: 10 August 2016 / Accepted: 7 March 2017

Abstract Privacy is a critical challenge for corporate social responsibility in the mobile device ecosystem. Mobile application firms can collect granular and largely unregulated data about their consumers, and must make ethical decisions about how and whether to collect, store, and share these data. This paper conducts a discourse analysis of mobile application developer forums to discover when and how privacy conversations, as a representative of larger ethical debates, arise during development. It finds that online forums can be useful spaces for ethical deliberations, as developers use these spaces to define, discuss, and justify their values. It also discovers that ethical discussions in mobile development are prompted by work practices which vary considerably between iOS and Android, today's two major mobile platforms. For educators, regulators, and managers interested in encouraging more ethical discussion and deliberation in mobile development, these work practices provide a valuable point of entry. But while the triggers for privacy conversations are quite different between platforms, ultimately the *justifications* for privacy are similar. Developers for both platforms use moral and cautionary tales, moral evaluation, and instrumental and technical rationalization to justify and legitimize privacy as a value in mobile development. Understanding these three forms of justification for privacy is useful to educators, regulators, and managers who wish to promote ethical practices in mobile development.

Keywords Corporate social responsibility · Occupational ethics · Privacy · Qualitative analysis · Technology ethics

✉ Katie Shilton
kshilton@umd.edu

Daniel Greene
dgreene@microsoft.com

[1] University of Maryland College Park, College Park, MD, USA

[2] Microsoft Research New England, Cambridge, MA, USA

Introduction: Investigating Work Dynamics that Impact Privacy Reflection

Mobile technologies enable new forms of access to information and communication. But even as the capabilities of mobile technologies advance, many fail to reflect and support the values of their users. Studies demonstrate a striking discord between user values such as privacy and implementation of these values in mobile technologies (Martin and Shilton 2015). Encouraging the developers and technology firms responsible for shaping our increasingly sociotechnical world to consider corporate social responsibility and the ethics of their work is an ongoing, unmet challenge (Brusoni and Vaccaro 2016). Building explicit ethical reflection into technology development is a goal of researchers (Miller, Friedman, and Jancke 2007; Spiekermann and Cranor 2009; Verbeek 2006), regulators (Federal Trade Commission 2012), and many firms (Brusoni and Vaccaro 2016). There has been little research, however, to understand how developers make choices between technical features that support ethical values (e.g., privacy or fairness) over other values (e.g., efficiency or novelty). Workplace and organizational dynamics that impact ethical reflection and debate within technology development are not well understood.

This paper investigates reflection about an important ethical topic within the mobile device ecosystem: privacy. The necessity of "privacy" for mobile applications is

Published online: 28 March 2017

advocated by ethicists (Martin 2015), consumers (Martin and Shilton 2015, 2016), regulators (Harris 2013), and firms that recognize the link between privacy and consumer trust (Martin 2013; Pavlou (2011)). However, consumers, firms, regulators, and ethicists may understand "privacy" differently. Privacy can be defined as variously as technical data protection measures (Kelley et al. 2012); individual control over personal data (Westin 1970); appropriate data use in situated contexts (Nissenbaum 2009); or categories of harms to individuals and groups (Solove 2010). Mulligan et al. (2016) describe privacy as an "essentially contested concept," arguing that the definition of privacy depends upon situated practice, and that scholars must analyze how privacy is invoked and discussed across multiple contexts.

Understanding how privacy is debated and contested by technology developers is particularly important for mobile applications. Mobile data are a rapidly growing form of personal data. In the USA, for example, mobile application usage grew 90% and contributed to 77% of the total increase in digital media time spent by consumers between 2013 and 2015. Two out of every 3 minutes Americans spent with digital media was on a mobile device, and mobile applications constitute just over half of those minutes (comScore 2015). During these activities, mobile applications collect personal data to facilitate both services and advertising. The data they collect may also be sold to advertisers, shared with strategic partners, given to analytics companies, or siphoned by hackers. The mobile application developers ("devs") frequently responsible for making decisions about user data range from hobbyists to consultants to independent contractors to employees of multinational corporations (VisionMobile 2016). Low barriers to entry enable a vibrant but deprofessionalized development ecosystem (Cravens 2012), and surveys of application developers have revealed that many lack knowledge of current best practices for privacy and data protection (Balebako et al. 2014). Devs also rely on distribution by two major international platforms: the Apple App Store and Google's Play Marketplace (VisionMobile 2016). While digital platforms regularly present themselves as neutral intermediaries for user content, the corporate actors that build platforms actively shape the content they host through both technical design decisions and policy mechanisms (Gillespie 2010). In mobile development, such shaping includes attention to privacy, and devs must navigate the privacy rules and regulations of these application platforms.

Current US approaches to regulating data protection in the mobile ecosystem rely on privacy *by design*: approaches that encourage developers to proactively implement best-practice privacy features to protect sensitive data (Cavoukian 2012; Lipner 2004). Privacy by design emphasizes corporate social responsibility and positions developers and mobile application firms as ethical agents, responsible for deciding how to define and operationalize privacy. But we don't know what factors motivate developers and firms to implement privacy or data security features when faced with disincentives such as longer development timelines, markets for personal data, and tensions between data protection and data-enabled services. If we can find development practices that encourage developers to define, and then design for, privacy, we can improve protections for sensitive mobile data.

The paper uses discourse analysis of developer forums to discover when and how privacy conversations, as a representative of larger ethical debates, arise in mobile application development. We focus on one factor that can impact the way that ethical debates unfold within firms: the link between ethics awareness and *work practices*. This paper asks: What work practices trigger discussions of privacy among developers? And how do these practices vary among mobile platforms (Google's Android and Apple's iOS)? It discovers that ethical discussions in mobile development are prompted by work practices which vary considerably between iOS and Android, today's two major mobile platforms. iOS developers spark privacy conversations when they navigate App Store approval and encounter technical constraints imposed by the platform. In Android, navigating permissions, user requests, and the privacy features of other developers all serve as levers for privacy discourse. And in both ecosystems, reviewing analytics and interacting with third parties trigger privacy discussions. But while the triggers for privacy conversations are quite different between platforms, ultimately the justifications for privacy are similar. Developers for both platforms use moral and cautionary tales, moral evaluation, and instrumental and technical rationalization to justify and legitimize privacy as a value in mobile development.

Background: Ethics in computing work

Researchers in business ethics, applied ethics, and technology ethics have investigated ethics in computing for more than 30 years. Work in business ethics focused on defining the needs and expectations of stakeholders such as firms and consumers in computing ethics debates (Drover et al. 2012; Martin 2015). Seminal work in computer ethics analyzed existing systems for biases and ethical import (Brey 2012; Friedman and Nissenbaum 1997; Guston 2011; Moor 1985). Work in ethics education focused on training computing engineers in relevant computer ethics (Herkert 2001; Hollander 2009). Work in ethical design focused on eliminating bias (Friedman and Nissenbaum 1997), achieving privacy by design (Spiekermann and

Cranor 2009), or encouraging sustainability (Froehlich et al. 2010).

Within this work, privacy is a value that frequently rises to the forefront of conversations about developers, consumers, and the platforms they use (Ashworth and Free 2006; Introna and Pouloudi 1999; Martin 2015; Urban et al. 2012). Privacy's status as an essentially contested concept (Mulligan et al. 2016) is illustrated within these debates. In the USA, policy definitions of privacy have centered on Fair Information Practices: a set of best practices for corporate data collectors that center on providing notice of data collection, choice for consumers to opt out, access to data upon request, data security, and redress of errors (Waldo et al. 2007). Privacy-sensitive consumers can (theoretically) opt out of data collection or request to see their data. However, empirical research has documented the failure of notice and consent (Cranor 2006; Leon et al. 2011; Martin 2013) and shown privacy to be less dependent upon individual preferences than social norms (Martin and Shilton 2015, 2016). This research fits theories suggested by Cohen (2012) and Nissenbaum (2009, 2015), which suggest that context-based norms, and people's understanding of their roles within those contexts, are critical to privacy expectations.

Nissenbaum's theory of privacy as *contextual integrity* is particularly influential. Nissenbaum describes how definitions of private information vary according to social context. Design implication of Nissenbaum's theory includes first that movement of information between contexts can violate contextual integrity and second that the regulators and designers of environments that process sensitive information must consider appropriate data uses based on contextual variables such as roles, norms, and information flows. Contextual integrity encourages researchers (and developers) to focus less on constructing definitions of privacy that cross contexts, and to instead focus on how privacy functions for different people in different spaces, to inform user-sensitive design and policy. This motivates the present research: investigating *how* privacy works in different mobile development ecosystems, and how an ecosystem's actors understand and negotiate privacy.

To investigate how privacy works in an information ecosystem, it is important to understand the ethical cultures that shape emerging technologies. In previous work (Greene and Shilton in press) we have analyzed the ways that mobile application developers define privacy. We found that iOS developers largely defined privacy according to Apple's guidance, which relies upon consumer notice and consent, while Android developers define privacy as a set of defensive features through which developers respond to threats from actors ranging from nosy friends to Google itself. The current analysis extends this work to determine *when and how* privacy discussions and decisions emerge within application software development, and what encourages these discussions and decisions to take place. Studying the emergence and character of privacy discussions necessitates studies of *work practice*, long important within organizational studies (Cetina et al. 2001; Davenport and Hall 2002; Orlikowski 2007), to understand how actors collectively create behavioral norms through social and material interactions. For example, Gurses and van Hoboken (2017) have written about the ways that a shift from "waterfall" to "agile" software development practices has influenced how privacy is defined and governed in software. In previous work, Shilton (2013) has written about the ways in which particular work practices common on software development teams, termed values levers, can raise discussions about social values and influence decisions about values such as privacy. Values levers operate by making room for values discussions within technical work. In turn, these discussions make social values relevant to technical work and encourage ethics-oriented design choices (Fig. 1).

This paper expands on the concept of values levers by considering the mediating role of platforms: corporate actors that, because they control access to markets, have the power to influence the work practices of an entire industry (Gillespie 2010). We contrast two platforms—iOS and Android development—with similar technical challenges, but different regulatory practices and development ethos. We investigate what values levers exist in these ecosystems by finding work practices that trigger privacy conversations. Opening privacy conversations is only the beginning of the story for privacy by design, however. Once the conversation is raised, the way that the conversation proceeds matter to development. A recent study contrasting iOS and Android applications found that 73% of Android apps tested, and 47% of iOS apps tested, reported user location. In total, 49% of Android apps and 25% of iOS apps shared personally identifying information (Zang et al. 2015). These numbers illustrate broad sharing

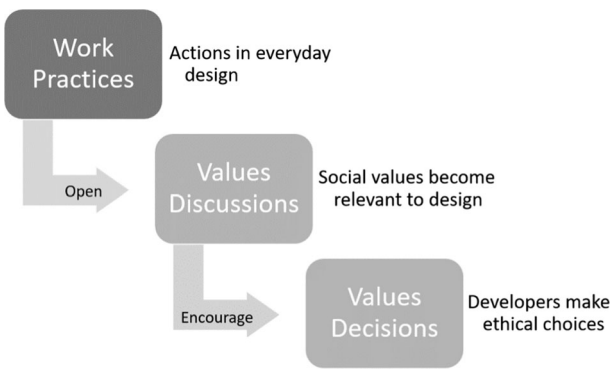

Fig. 1 Values levers in development work

of personally identifiable information generally, but also that such sharing is noticeably more prolific in Android. Such findings invoke questions of *why*: Why is privacy so differently enacted within Android and iOS ecosystems? After outlining our methodological approach (Sect. 3), we answer this question. Section 4.1 describes value levers for privacy in the iOS ecosystem, Sect. 4.2 contrasts values levers for privacy in the Android ecosystem, and Sect. 4.3 describes levers common to both ecosystems. Section 5 describes the justifications for privacy shared across ecosystems. We close with a discussion of why these values levers, and values conversations, matter to design.

Method: Discourse Analysis

To understand how privacy discussions are triggered and unfold in each development ecosystem, we have undertaken a critical discourse analysis of mobile developer forums. Critical discourse analysis is a qualitative method for analyzing the way that participants talk about their social practices (van Leeuwen 2008). Critical discourse analysis looks for the ways that written texts (in this case, forum posts) describe social practice by representing social actors, action, time, space, legitimacy, and purpose. Critical discourse analysis allows us understand how a value like privacy gains legitimacy in mobile development and further understand the work practices that actors link to that legitimacy.

We drew data from two online forums where mobile application developers meet to discuss their work. The iPhoneDevSDK forum supports iOS developers and features such topics as code sharing, programming tutorials, open discussion, and marketing guidance. Unlike other Apple-related forums, it focuses on development advice and guidance rather than device reviews or product announcements. It is also not run or moderated by Apple and does not require an Apple-issued Developer Key to participate. Participants therefore appear to be more diverse than those in Apple's official forum, in terms of experience and purpose for participating. For example, sometimes non-dev participants (e.g., advertising network representatives searching for potential clients) participate in forum threads.

The second forum we studied was XDA, which includes within it the largest and most active Android developer forums on the English-language web. It features many of the same technical topics as iPhoneDevSDK, but widens its participant base to include the consumers and hobbyists reviewing devs' products, suggesting technical developments, and debating industry news. XDA featured more diverse participants in terms of professional background and geographic location, drawing participants with all levels of expertise and interest from all over the world, and had a wider variety of discussions about non-technical topics.

In each forum, we found and analyzed threads based on the value that was the focus of our study: privacy. We chose privacy because our previous work pointed to privacy as a value frequently discussed within technical communities that also *stands in* for less-frequently discussed values such as equity, fairness, and justice (Shilton 2013). We searched for threads which contained the term "privacy" and chose to analyze those that included a discussion of privacy (that is, at least two replies discussing privacy). We discarded threads where "privacy" was used as a keyword in an advertisement for an app or instances where devs posted job ads and promised privacy for job applicants. On iPhoneDevSDK, we found 155 results in June 2015 (ranging from 2009 to 2015) that fit these criteria. We exported those results to the online qualitative data analysis software Dedoose as HTML files for coding.

XDA is a much larger community. To narrow our search and ensure each result contained active discussion, we limited our "privacy" search to threads containing at least two replies, housed within either XDA's App Developers, Android Wear, or Android Development and Hacking forums (with the vast majority of results coming from the last). The search was performed in October 2015 and yielded 485 results. To balance our analysis with that of the smaller iPhoneDevSDK, we sampled every third result and exported the relevant thread to Dedoose as a PDF for coding.

Both authors read through the full dataset to generate a set of initial thematic codes. These codes initially focused on privacy definitions, as well as any discussions of work practices. We then divided the dataset in half and coded threads separately, reviewing each other's codes in weekly meetings to ensure mutual understanding and thematic coherence. During this process, the code set grew to include pressures against privacy (such as data collection and personalization needs), ways that privacy was authorized and legitimated, and conceptions of other actors in the ecosystem (Apple, service providers such as SDKs, and users). Our final code set comprised 13 codes and 39 subcodes.

To explicitly find values levers in each ecosystem, we identified places where discussion of work practices (such as gaining App Store approval or dealing with user requests) co-occurred with discussions about privacy. We then analyzed the relationship between the two codes. Could the work practice be said to spark or trigger the discussion of privacy? If so, we identified these work practices as values levers.

Our university's IRB certified that the forum data gathered here qualified as public data and thus did not

qualify for further IRB review. However, we believe that directly quoting participants violates the contextual integrity of the forum space; forum participants may not expect their posts to be used for research. To minimize this violation, we have altered participant handles and slightly altered quotations within this paper to reduce the ease of searching for specific exchanges. Alterations preserve the original meaning of posts, and all analyses were conducted on the original, unaltered quotations. We have also announced our ongoing work on the forum and offered a survey to participants (currently under analysis as future work) to gather information on their professional backgrounds and values.

Levers for Privacy Discussions

Our research sought to understand triggers, or values levers, for discussions of privacy among iOS and Android developers, and how differences in work practices between platforms might lead to different values levers in developer discussions. Answering these questions highlighted significant differences between the two ecosystems, including different work practices, licensing models, and development cultures associated with Android and iOS software. In turn, these differing work practices, licensing models, and development cultures impacted both the frequency and tenor of values discussions in iOS and Android development forums.

Values levers in iOS: App Store approval and technical constraints

The major lever for privacy discussions for iOS developers was navigating Apple's approval process. Apple, unlike Android, has a gated marketplace: Applications must be approved by a team within Apple before they are distributed via the App Store (Spencer 2016). Although the App Store opened in 2008, Apple published the first version of their *App Store Review Guidelines*—their official policy guidance for developers—in September 2010. Discussions threads about privacy spiked during 2011, as shown in Fig. 2:

Most of these 2011 privacy discussions were trying to unpack the guidance newly provided by Apple.[1]

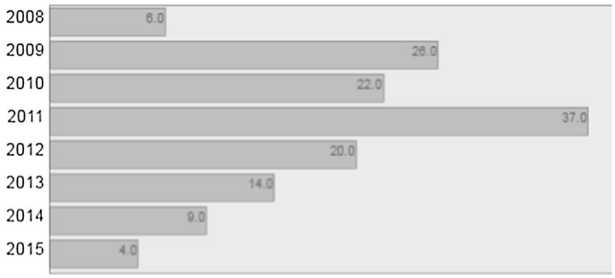

Fig. 2 Threads on iOSDevSDK containing substantive privacy discussions

Indeed, in all years represented in our data, trying to navigate the Apple App Store approval process was the single most common trigger for privacy discussions. Many discussions were triggered when someone wrote to get advice about why an app was rejected. In a March 2010 thread (before the launch of the *App Store Guidelines*) forum newbie LudoJoy described his "small business in France" that had just launched its first iPhone app.

> LudoJoy: … Our app was simply to record outgoing calls. In fact, it's the same feature as [an already existing app]. Our app was rejected, because "Apple doesn't allow call recording." So, it seems that a feature can be allowed for some, but not for others!

He went on to bemoan the fact that his small company couldn't risk ongoing rejections from the App Store. Despite the lack of official policy guidance that would have banned recording outgoing calls, other developers were critical of LudoJoy's assumptions. Frequent forum participant DrD invoked moral arguments, implying that LudoJoy should have known better:

> DrD: You should have known that recording app will be rejected. Don't look at others - others might rob a bank and get away with it. I can't imagine how on Earth Apple allowed that other recording app that you mentioned.

In this example, a new developer's frustration with the App Store approval process triggered discussion about the ethics of call recording. For the new developer, Apple's position may have seemed arbitrary, but a veteran forum participant emphasized that privacy was a moral obligation enforced by Apple.

A less-common work practice that triggered privacy discussions among iOS developers was encountering, and trying to resolve, a technical constraint. Developers stumped by a technical maneuver would write in for advice. For example, in a September 2011 thread, brand-new user 33cd3 wrote in, frustrated by video capture constraints:

[1] Privacy discussions spiked in 2011 but then rapidly decreased year over year. We believe this is because once a question about Apple's privacy policy is answered, the exchange is preserved in the forum indefinitely and future participants interested in the same question can find the answer by searching instead of asking. Indeed, on the rare occasions a policy question that was already answered elsewhere on the forum came up, we saw veteran participants linking newcomers back to the relevant thread.

> 33cd3: i want to capture a video from the iphone camera …without pressing any button and the user dont even know, without open the camera view so the user dont know that camera is working…it is possible? Tnx

Immediately, experienced users piled on with warnings that this was not only impossible, but unethical. Frequent poster Meredi92 began the responses:

> Meredi92: Unlikely! Its not something i have looked into doing, but based on what most people complain about i think that filming from their device without their knowledge would be a big no–no. It would definitely stop me from downloading an app if i saw/knew about that sort of functionality.

After Meredi92, an even more experienced poster, Smithdale89 chimed in: "I think it would be possible." He then gave a set of recommendations for technical videos that might help 33cd3 figure out the technical constraints. But then he added: "Definitely a huge invasion of privacy though, IMO, and I doubt apple would approve it." In this case, Smithdale89 seems to think access is technically possible, but won't be allowed by an Apple reviewer.

The thread took an interesting turn when original poster 33cd3 replied to the multiple chiding responses rather defensively: "Hmmm. No, spying or any other 'bad things' is not the point of this app. It's for cool idea." Meredi92 posted the final word in the thread, positing an approach that mixed respect for ethical norms with a good dose of pragmatic advice:

> Meredi92: Unfortunately its not just about a cool idea. People generally won't look past the fact that you are doing something without their knowledge to see that cool idea… I'm sorry that it will affect your app, it is a shame that these things happen - clashes between a great idea and an invasion of personal privacy. Its a fine line to walk, and without huge amounts of awesome lawyers and a stockpile of cash its a line that is best avoided if at all possible.

Meredi92 illustrates the (deontological or rule-based) belief that a "cool idea" doesn't outweigh an ethical violation. The entire exchange illustrates the ways in which what was initially posed as a technical constraint can transform into an ethical deliberation. 33cd3 was blocked by a technical constraint when he couldn't figure out how to implement automatic video recording in the iOS operating system. Reaching out to other developers to surmount the constraint instead generated an ethics discussion about whether the ends (the "cool idea") justified the means, with community consensus erring on the side of privacy protection.

Values Levers in Android: Permissions, User Requests, and Product Differentiation

Android developers engage in some work practices that differ from those in iOS, creating a different set of values levers in this ecosystem. A fundamental difference between iOS and Android is that Android is an open-source project. This means that Android developers may modify all or part of the operating system, making Android highly customizable. The platform therefore imposes fewer technical constraints on developers, as developers can "fork" the code to modify the platform if there's a constraint they wish to circumvent. And while individual developers of Android applications can choose whether or not to open source their products, open source is as much a political ideology as a licensing agreement (Kelty 2008). Many of the developers on XDA made the source code for their applications available to others to modify. This makes it easier for users of an application to become developers of a similar, forked application, and the line between "users" and "developers" was blurry in the XDA forums. Developers were also users of other Android apps, and developers often recruited their users to help them with open-source projects. Finally, Android lacks the stringent App Store review process that was so critical to prompting privacy discussions in iOS. While Android developers must agree to the Developer Distribution Agreement (Google Play 2016) and are asked to include privacy features such as a privacy policy and encryption for data in transmission, the agreement explicitly states that Google does not "undertake an obligation to monitor the Products or their content." Instead, Google reserves the right to remove (called "takedowns") violating apps from the store at their discretion. Interestingly, app takedowns were barely mentioned in the XDA forums. Though it is difficult to know for sure why a topic is *not* mentioned in the forums, we can speculate that takedowns occur infrequently enough that they do not serve as a significant barrier to development. Privacy discussions did arise in Android, however. Work practices which sparked privacy discussions included working with analytics (as in iOS), as well as analyzing app permissions, interacting with users, and differentiating products for the crowded market using privacy features.

In both Android and iOS ecosystems, *permissions* are the form taken by privacy notices to app users. When a user downloads or updates an app, they will be notified of the permissions for data access needed by the app. Users, in the form of highly skilled hobbyists, were much more of a presence in the XDA forums than on iPhoneDevSDK. "Highly skilled" in this context most often meant those who could "root" their phones, which often voided the warranty but gave users the ability to act as administrators

on their own device, use the command-line interface, and adjust the operating system to fit their needs. Because hobbyists served as early testers for many of the apps posted on XDA, discussion of permissions was much more prominent. Notifications about permissions, particularly when installing apps, served as a trigger for privacy discussions. Sometimes this was phrased as a simple critique of an app. In a November 2010 thread devoted to an iPhone game which a developer had ported for Android, senior member OrganizedSir advised: "…until the developer can explain why this game requires access to the contacts, i advise no one to download it." Access to a person's phone contacts—their default social network—was considered sensitive and unnecessary for a simple game. Other forum participants chimed into agree:

> Boodles [senior member]: exactly, i'm holding off as well. doesn't even look that fun anyway.

> Gabu [junior member]: This. Why do 90% of the thread's posters seem to ignore, or fail to recognize this? Do people not care about privacy anymore?

Not only was the game condemned for requiring what participants understood to be too-permissive permissions, the state of user awareness of privacy itself was brought into question by the many forum posters who did not seem alarmed by the necessary permissions.

Permissions also served as a marker of app quality in an ecosystem in which it could be tough to judge trust and quality. For example, developer AttaAlla started a pleading 2012 thread titled "[Q] Why users do not use my app!!! (even with good rates)," to try to understand his app's lack of popularity.

> AttaAlla: Do Guys see any problem in my app? Do I have design problem? Do you find this app not useful?

Participants gave AttaAlla honest feedback on problems with his app, ranging from font choices to permissions. Permissions was an oft-repeated theme, brought up by at least six different posters in the thread. For example, senior member Polorabbit gave a list of reasons, among which were both permissions and a lack of privacy policy (as well as several culturally coded reasons delineating trust or lack thereof):

> Polorabbit: To sum it up: Simply too many functions and permissions. This is ridiculous. … No privacy policy of any sort. English is sub par. Too many typos. Design judging from screen shots is decent, although sparse. Comic Sans MS font still present as I can see. From all this, I wouldn't install your app. In the state it is, I would fear for my personal data and information.

Senior member rab2422000 chimed into agree:

> rab2422000: From what I see my comments are similar to the others - too many permissions, slightly amateurish design, ugly font, too big for a productivity app.

Requesting too many permissions was repeated throughout the thread as an indicator of poor quality or unprofessional design. In an ecosystem reliant on trust in other developers, these signals were important to hobbyist users. Discussing permissions served as a values lever for conversations about trust and data use.

As demonstrated in the discussions about permissions, a distinctive feature of the Android ecosystem was the tight communication links between app developers and skilled hobbyists. The XDA forums provided direct communication between developers and one potential user base and blurred the lines between the two. As a result, a frequent lever for privacy conversations on the forum was user requests for new features. For example, forum member yajinni posted the following request for a new feature on a 2013 thread discussing a time-saving app launcher:

> Yajinni: Hello, is it possible to add to this something that tracks your most USED apps? Like a list of apps you use the most instead of your most recent list?

The creator of the app launcher, a senior member called Roshga, replied:

> Roshga: That will require to keep track on what apps you're launching and counting those numbers… I'm not a fan of going into someone's privacy so I don't think we'll implement that.

In this example, the product developer recognizes the privacy implications of a feature requested by a user. But hobbyists could also alert developers to privacy concerns. Hobbyist users were often sensitive to contextual privacy concerns that developers, who worked across multiple contexts, might miss. For example, in a 2013 thread, senior member MildlyTroubled used the forum to question One_for_all, a junior member who created a painting app for children:

> MildlyTroubled: While I've never really been a freak for privacy and permissions, I do question why there's a children's app that has access to my child's GPS coordinates and my account data [lists permissions from app download screen]. That particular set of permissions makes me feel like someone's going to drop in, scoop up the kid, then with the account access email, tweet, or facebook me a ransom note.

One_for_all was swayed by MildlyTroubled's argument:

> One_for_all: Thank you for your comment. In the recently published updated version, we have removed the unnecessary permissions. You can now enjoy the new version without worrying about privacy. Many thanks, again!

The XDA forum provided an easy way for developers to interact with expert users of their applications, and it was often these highly skilled hobbyists who were most aware of privacy concerns when downloading and using an app. This interaction formed a values lever that helped to surface privacy conversations.

A large proportion of the privacy discussions on XDA took place on threads promoting apps which advertised specific privacy features as a way to differentiate a new product. A characteristic of the open Android marketplace is that any existing application could be modified by an interested developer to create a privacy-centric version of that application, resulting in alternate, privacy-centered versions of popular games, productivity apps, or even entire operating systems. Creating a privacy feature allowed lone actors interested in privacy to differentiate their products in a crowded marketplace and introduced a broader ethical conversation into the XDA forums.

While we couldn't necessarily analyze the personal values that went into creating those apps, threads supporting these privacy-featuring apps became a notable site at which XDA members—both devs and hobbyists—discussed and justified privacy. Specifically, privacy was discussed as a feature which could support the personal and political values of highly skilled users who could root their phones and install complex systems. Privacy threats (often from the government or the large corporations who built popular apps) brought devs and hobbyists together, and devs used their skills to thwart those threats.

For example, senior user Christoph31 set up a 2013 thread to discuss PDroid, a "a ROM-hooked [a custom operating system] privacy protection of your personal information and data" that is meant to "let you set per-app access rights to your private information." He wrote:

> Christoph31: This shall be a pure SERVICE thread to all users and friends of Android that care about their privacy. We (users & friends of xda-developers, PDroid & AutoPatcher) help you patching your ROM so that you can use your apps and games under privacy protection.

This effort stemmed from an earlier 2011 thread set up by senior member Sywat which polled the XDA community as to whether they would use such a service. In total, 162 respondents indicated that they would use it, while 4 indicated they would not. Echoing the poll, the hundreds of responses in the thread were uniformly positive, along the lines of senior member Havoc's response:

> Havoc: Please release this ASAP. We really need better privacy tools on our android phones! Google isn't helping by not giving the option to revoke permissions for applications.

Privacy-protecting technical features built as a means for product differentiation, whether designed into new operating systems or individual apps, were the most frequently coded lever for inspiring discussion about privacy in the XDA forums.

Shared Values Levers: Analytics and Interacting with Third Parties

Though the iOS and Android ecosystems supported many different work practices, there were also work practices common to development for both platforms. Application developers in both platforms did market research, modified their applications, and evaluated their success using *analytics*: the data provided by the platforms, or outside parties, to help developers understand their users' demographics and behaviors. And developers in both platforms marketed and monetized their applications by interacting with third parties such as advertising companies.

One lever for privacy discussions in both Apple and Android ecosystems was engaging with the analytics that helped them understand user behavior within their app. Often looking at this data or discussing data collection made privacy concerns explicit and concrete to devs. For example, in a July 2013 iPhoneDevSDK post, a user who was new to the forum, but already quite active, posted:

> CoderPro: I'm constantly thinking of ways to do a better job promoting my app, and just recently I found out about the Google Analytics Tool… How exactly does it go about sending the information to the Google server and how often? Is this something that might upset users because of privacy concern?

CoderPro considers privacy to be a primary concern for evaluating use of a new metrics tool. He goes on to specify that he's done some searching about the tool, but hasn't found the opinions he wanted. He's hoping that more experienced participants can recommend the tool. Three respondents to the thread, all experienced users but infrequent posters, generally praise the tool, including a real-time dashboard "where circles appear on a map every time someone starts your app." Because no one explicitly addresses privacy concerns, CoderPro brings them back up: "How do you go about asking users if they're ok with you

collecting data? Or do you even bother?" User Joseph replies "It only collects non-personally-identifiable data so I don't bother to let people know." This response seems to satisfy CoderPro, as there is no additional follow-up.

In a different example, a May 2015 iPhoneDevSDK discussion was spurred by a developer who had been playing with analytics provided by the App Store. This prompted a discussion about whether users could or should be automatically opted into metrics tracking. Relatively new user PrimoTM began the discussion with a caveat:

> PrimoTM: Also note that these [App Store analytics] stats are only for apps … where the user has agreed to share data with developers. I have no idea what percentage of users agree, but I don't think it's high.

More experienced user Alifor responds, confused, assuming all users were incorporated into the App Store's analytics:

> Alifor: Will this not be automatically accepted by a user? If not, Apple shows us incorrect data which we cannot rely on.

Dev69, an experienced participant with over 3000 posts in the forum, responds directly: "Don't think so due to privacy issues," followed by a winking emoji. Dev69 implies that Apple wouldn't automatically opt users into analytics because of privacy concerns. In both exchanges, interacting with analytics was the prompt to think through how *users* might respond to those analytics, prompting discussion of privacy concerns.

Discussion of analytics sometimes prompted privacy discussions in the Android ecosystem, as well. Developer Aryray started an XDA thread to advertise an app that provided custom boot screen animations. Adroc, a junior member, wrote to the developer to ask why a data connection was needed to run the application and to request an offline-accessible version. Aryray defended his choice by citing the analytics engine he was using:

> Aryray: Im collecting data to see how many people are using my app, and you need a data connection to use it.

This prompted junior member JenJAM to critique his choice:

> jenJAM: From a user privacy standpoint, I really hate user-analytics. I don't like applications using my (limited) data plan to accumulate data about my behavior. I find actions like this invasive and in violation of my privacy. Please give users an option to turn this off.

JenJAM was not the only concerned user; several other participants chimed into request that users be given the option to turn off analytics tracking. In response, Aryray conceded the technical point, but not the ethical one. Responding directly to JenJAM, he wrote:

> ARyray: I added that to my next release, if no data connection is available you will need to connect to wifi.

This concession allows users to avoid using their data plan, but not to avoid tracking. This exchange highlights a common tension that we will explore in more depth below: instrumental or technical rationalizations for limiting data tracking were often more convincing to developers than moral or ethical arguments.

A work practice related to the analysis of metrics was interacting with third parties, particularly software development kits or SDKs. "SDKs" was a term used frequently in the forums to refer to companies that collect metrics or provide advertising services. As developers considered interacting with SDKs, or interacted with them directly, they often considered the implications of doing so. Privacy was a frequent concern among those implications. For example, in a March 2009 thread on iPhoneDevSDK, Rooster100, a relatively infrequent poster, asked a question on a thread devoted to SDK implementation:

> Rooster100: If you use either Company Y or Company Z are you supposed to be disclosing this to your users? It's basically spyware in a way right?

Frequent poster Calimba wrote a measured reply pointing out that the analytics tools were "sandboxed" and therefore had "access to very limited information without the user's consent." But Rooster100 wasn't convinced:

> Rooster100: When I first heard of these services I was planning to use it. I showed it to a couple of buddies of mine and the first thing out of their mouths were spyware bla bla bla.

The invocation of spyware was enough to encourage the VP of marketing at Company Y to chime in, in a post signed with his name:

> VP: As Calimba points out, you may disagree with the notion of collecting user data altogether, which we respect. It is worth noting that no data provided to companies is personally identifiable, as is strictly stated in our Terms of Service. We take privacy very seriously.

Similar examples occurred in the XDA forums, as well. A March 2010 thread started by senior member EddyNC and titled simply "Android Privacy" began:

> EddyNC: Hi all, I have a major concern about privacy and all the 3rd party data collectors…A lot of apps

> are uploading user info and stats to companies like [Company X], [Company Y] etc. … I want the option to choose whether or not this kind of info gets collected and distributed. I've looked into this issue on the android platform, and it seems like there's no option other than not to install the app.

This inspired a lengthy discussion of technical means to block particular companies, existing apps that might help the original poster avoid monitoring by third parties, and the creation of lists of offending third parties that could be shared with the broader XDA community:

> Senior member Fabian: Could you please post the host-file or the addresses/ip's of the companies your gonna block? they should be of interest for everybody here.

The XDA community was inspired to troubleshoot solutions to third-party privacy challenges by EddyNC's initial post.

On threads devoted to two different platforms, Rooster100 and EddyNC both express fears about putting trust in third parties to manage analytics and data about their users. And the third parties involved in this ecosystem recognize this concern and seek to mitigate it in these threads.

Justifying Privacy: Cautionary Tales, Moral Evaluation, and Rationalization

Once we had established the work practices which opened privacy discussions within the forums, we turned to analyzing the tone, tenor, and content of privacy discussions in Android and iOS development. How did participants in the forums justify privacy as a value, especially in the face of competing values? We turned to analyzing how forum participants justified privacy as a legitimate design value or user preference, reviewing arguments that legitimated respect for privacy. Building on categories suggested by van Leeuwen (2008) for a critical discourse analysis approach, we identified the telling of stories to illustrate good and bad consequences of ignoring privacy (what van Leeuwen identifies as moral and cautionary tales); moral arguments for privacy (what van Leeuwen identifies as moral evaluation); and technical and instrumental arguments for the importance of privacy (what van Leeuwen identifies as rationalization). All of these forms of justification appeared in both Android and iOS ecosystems.

Developers often told stories to legitimize privacy. These stories took the form of moral tales, which identified particular actors or classes of action as bad, as well as cautionary tales, in which actors are punished for their immoral or illegal actions.

A frequent moral tale was the invocation of either "spyware" or "spam." Both spyware and spam were invoked in stories to represent immoral software or immoral actions by software, and devs took pains to distinguish their apps from spyware and spam. As btc2020, who identified as "new to iOS development" posted in a 2011 thread, he began to ask other developers about the acceptability of an always-on app that could send texts in the background:

> Btc2020: This will not be spyware, and the user will be fully aware of this feature if they launch the application.

User Dom had the first reply:

> Dom: I doubt that you can automatically send texts without user action even if the user is fully aware of it. Too much room for spam, I mean I know your intentions aren't to send ads out but some people aren't as honest.

Other users agreed that it couldn't or shouldn't be done. Original poster btc2020 wrote back to let them know he accepted their concerns:

> Thanks everyone. I guess it can be done [through alternative technical means] … though I do understand the privacy and spam concerns.

In this conversation, it was clear that both the original poster and the other users in the thread were using both spyware and spam to evoke socially undesirable activities.

"Spyware" retained similar moral loading in the Android ecosystem. In a 2013 thread discussing a Chrome extension, member Lekenstine flagged a download posted to the forum, writing:

> Lekenstine: I don't know WHO that developer is, but that version… includes code to track you (=**spyware** in my eyes).

Member Darsis wrote back to ask for clarification:

> Darsis: what exactly do you mean by "code to track you"?

Lekenstine's reply again invoked the cautionary tale, defining spyware as software that executes an unnecessary privacy violation:

> Lekenstine: Besides tracking the installation event, you also track page views (when the options page is opened, and the background script is loaded). This effectively means that you also track when the user start his browser. An unnecessary privacy violation imo which also qualifies for spyware.

Cautionary tales frequently informed other devs of potential bad outcomes that could result from particular forms of data collection. Some cautionary tales imagined very concrete legal consequences for bad privacy decisions. For example, a 2009 iPhoneDevSDK thread drew devs' attention to the potential for privacy lawsuits. Registered user John2367 began the thread by sharing a news article from *PCWorld* with a grim message:

> John2367: This article is a warning for anyone that who do not play by the rule. From *PCworld*: "Lawsuit Claims IPhone Games Stole Phone Numbers": "a pending class-action lawsuit filed against the devs, claiming that each of the company's games took advantage of a 'backdoor' method to access, collect, and transmit the wireless phone numbers of the iPhones on which its games are installed"…The lawsuits are real and it will cost you a lot if you can not defend it or if you can not afford a lawyer. Let's begin the guessing game, how much "punitive damage" the lawyer want? 1 millions? 2 millions? May be declare bankruptcy before it finalized.

Lawsuits weren't the only legal consequence used as a cautionary tale: Developers frequently notified each other (correctly or not) that particular kinds of data tracking were illegal. For example, in a 2013 XDA thread advertising an Android app called "Spy Your Love," advertised as the "best cheating prevention and detection mobile app," member Monicar John wrote a response to the developer:

> Monicar John: To some extent, [your app is] useful, but it's illegal! Are you going to implement some sort of location tracking? … I think it will be a good feature for your app, but is illegal to spy on your love without permission.

Extremely prolific iPhoneDevSDK poster Duncan, responding to the 2011 thread critiquing video capture discussed above, warned:

> Duncan: Indeed, I think I would sue if I found out an app was filming me without my knowledge or permission. If you upload that video that would probably be felony invasion of privacy. (Read prison time.)

Illegality served as a cautionary tale for developers who would build such apps, or users who might use them.

Another genre of cautionary tales used bad actors as a tactic to encourage attention to privacy. While these were occasionally vague references to data falling into the "wrong hands," the imagined bad actors were frequently quite specific. As senior member (☺) wrote in a 2011 XDA thread devoted to discussing Android security:

> (☺): I recently got my Samsung Galaxy S4 9505 and I WAS FKN SHOCKED!!! Android 4 Smartphones became a super spy machine - it gets everything from you, I mean EVERYTHING! ALL YOUR INPUT DATA! Even your face, your voice, your photos, your messages, your photos/videos, your private life AND the private life of your family & friends!… Who can get this data? Of course and foremost google (and all companies behind and in google), but also a lot more: Samsung, Sony, HTC and every other mobile-phone-producer…

Phone companies were not the only imagined bad actor. In a 2011 iPhoneDevSDK thread, new user Lisglympt, who identified as a European iOS dev, wrote:

> Lisglympt: We are not located in USA or EU. We take privacy VERY seriously. I have denied to comply with subpoenas issued by US courts. None of the big companies in USA seem to do that. We have customers in the Middle East and other places to whom this is the main reason to choose [our application]. This last point is something I have been struggling to get through, but the latest Wikileaks/Twitter subpoena case has given me some traction. It is safer to keep your data outside USA. People should and will take privacy more seriously in future.

The invocation of the US government as a privacy adversary prompted another iOS dev, registered user MichaelS, to respond:

> MichaelS: That [privacy policy] should be the primary focus of [your] web page, in my opinion. …The title should be "We are the Swiss Bank of Email Providers." Seriously. People will get what that means in terms of their email security.

As MichaelS's encouragement demonstrates, government surveillance was a convincing bad actor that served as an effective cautionary tale, legitimating privacy for developers.

Some developers went beyond cautionary tales, which implied bad results for bad actors, and additionally made *moral* evaluations, in which invoking privacy was enough to shut down whole lines of development. As van Leeuwen describes it, moral evaluations represent:

> …the tip of a submerged iceberg of moral values. They trigger a moral concept, but are detached from the system of interpretation from which they derive, at least on a conscious level… (2008, p. 110).

We coded tip-of-the-iceberg moral evaluations throughout the forums. Over and over again, devs on both platforms used the figure of *privacy* as a reason unto itself

for action, as in this 2010 iPhoneDevSDK exchange between two registered users:

> sparkdd: Hi, I develop an app that needs to get the phone number of the device. So do you know the function that returns the iPhone phone number? Thanks
> octobot: U cant do that. The privacy concerns associated for that would be insane
> sparkdd: thanks

Privacy *was* the reason: it was enough all by itself, invoking moral concepts without having to go into the details of why and how. Invoking privacy could be enough to shut down a whole exchange.

Developers also used forum conversations to take strong moral stances regarding privacy. In a 2012 iPhoneDevSDK thread begun by a developer who wished to use a particular form of location data, new user Iowyp took the following stance:

> Iowyp: That's just impossible with the data from iTunes connect. The only way to do so should be sending you the device location at launch of the app but that would be against user privacy and therefore should not be done.
> Iowyp later clarified his stance further:
> Iowyp: That statement was my opinion not a policy related statement. I don't think it's right for devs to access that data if the app does not require it. But, again, it's just a personal opinion.

Sometimes devs took other participants to task for poor moral calculations. Koolman, an iPhoneDevSDK participant upset with an advertising company for collecting what he deemed to be unnecessary address book information, wrote a 2012 response to a representative from that company:

> Koolman: As to your explanation, sorry but I just do not buy this. U don't tell why u need the AddressBook framework and [you say there's] no way to have your platform without it. Yes I saw that also [a competing company] requires it….. If your justification is that everyone does the same … It's like we steal cause many people also do steal. I'm still not buying this.

In the Android ecosystem, privacy was frequently legitimated as a personal value, rather than a universal moral value. Hobbyists or developers participating in the forum would express privacy as something they personally valued or wanted, as in this 2014 post from a junior XDA member:

> nusername: For privacy reasons I don't want Google to have my location information, even if they say it's "anonymous" it's possible to build a profile.

XDA senior member MrE, who chimed in on a 2011 thread polling users about whether they'd adopt PDroid, "the better privacy protection app" expressed his preference memorably:

> MrE: Am also interested in this app… Sounds very promising and I hope this will get ported for [my phone model], so I can get some freakin' privacy!

Moral reasons were not the only arguments devs used to persuade others to care about privacy. Some devs rationalized privacy as a market necessity, reasoning that users would abandon products that violated user privacy. In the 2011 thread discussed above about whether it was possible to capture video without users knowing, registered user Meredi92 wrote:

> Meredi92: Look, i havent looked into doing it, but based on what most people complain about i think that filming from their device without their knowing would be a big red light. It would for sure stop me from downloading an app if i saw/knew about that functionality.

This rationalization seems to imply that users would refrain from downloading an app if they knew about its data collection behavior, hurting sales.

In the Android marketplace, where privacy is a feature to be traded off against other features, rationalizations *for* privacy often had instrumental goals as well, such as saving battery life. In a 2011 thread titled "How can we keep Android from phoning home," senior member S_Magnolia praised the discussion:

> S_Magnolia: I think it is a very useful thread as it helps stop what I consider consumer abuse, and not to mention help free up resources like battery and memory on our Droid devices.

S_Magnolia unites "consumer abuse" (over what s/he sees as privacy concerns) with the instrumental purpose of freeing up hardware resources. Willy900wonka put it more dramatically later in the same thread:

> So let me understand this. I buy access to a network for my phone, which I also paid for. My location information, which is the result of my purchases is being used to generate income. So I'm allowing my spent cash to generate data and be leveraged to generate income. My information wouldn't exist without my investment in the technology, so I own it. I'm paying to be stalked!!!

Table 1 Values levers in the iOS and Android ecosystems

	Values levers						
	App Store approval	Technical constraints	Third parties	Analytics	Permissions	User requests	Product differentiation
iOS	●	●	●	●			
Android			●	●	●	●	●

Rationalizations *against* privacy often focused on convenience. In a 2015 XDA post suggesting new features for a messaging app, senior member Cyclonmaster wrote:

> Cyclonmaster: Good app. One thing SMS/MMS app nowadays lack is a backup option. If this app also have a built-in backup option to the cloud, this will be my ultimate app. …. If my phone lost/stolen, I can still retrieve my old sms/mms from cloud. (some say privacy issues, for me it is an option)

Cyclonmaster suggests that the convenience of cloud backup outweighs privacy concerns for him. This was a common opinion among forum participants. In a 2010 XDA thread devoted to privacy concerns in Google firmware, one senior member indicated that he would be avoiding phones with a "phone home provision" due to concerns about surveillance by corporations, thereby ruling out most Android handsets. Senior member kieranc responded succinctly:

> What's you not using an android phone going to fix? Sure, the world's heading to hell in a handbasket but that's no reason to use a crappy phone.

Discussion: Work Practices Matter to Ethical Deliberation

An important finding of this project for business ethics is that online forums can be useful spaces for ethical deliberations, as developers use these spaces to discuss, justify, and define values. For work that occurs frequently in distributed communities, fostering a culture of ethics can be a challenge. Understanding online forums as learning environments for occupational ethics enables ethics education beyond industry conferences, undergraduate and graduate programs, and other more traditional learning environments. For researchers, regulators, and managers interested in cultivating a culture of ethical debate and deliberation in mobile development (and other analogous forms of distributed work), online forums could be an important site of intervention. In addition, forums provide a space for platform providers—particularly firms which prioritize corporate social responsibility—to observe technical features and social processes that prompt ethical debates. Conflicts between the civic or social values firms espouse publicly and the values they act upon may alienate core users (Busch and Shepherd 2014). The values lever framework helps us recognize the technical and social features of platform environments that prompt ethical debates, and can help managers spot potential flashpoints before they develop into full-blown conflicts.

A second major finding is that ethical discussions in mobile development are prompted by work practices which vary considerably between the iOS and Android ecosystems. Table 1 illustrates the relative lack of overlap between values levers in the two ecosystems.

The rules, regulations, and cultural norms that govern each ecosystem impact day-to-day work practices for mobile developers. These differing work practices in turn shape the ethical deliberations engaged in by forum participants, addressing the question of why privacy is debated—and ultimately designed for—so differently between the two ecosystems. In iOS development, Apple's approval process and technical constraints inspire frequent privacy discussions among developers. This leads to design decisions that focus on meeting Apple's policy demands. Apple serves as a regulator, requiring baseline privacy-protection practices. We believe that this is why iOS applications are less likely to leak users' personal information (Zang et al. 2015). In Android development, developers differentiate their products in a crowded open-source marketplace through privacy features. Developers also regularly engage users and respond to user requests for new privacy features. These practices led to lively debates about aspects of "privacy" as diverse as the politics of NSA surveillance and Google's control over the Android ecosystem. While XDA did not exhibit as many explicit debates about privacy as did iPhoneDevSDK (and Android applications have been shown to leak more information than iOS applications), privacy discussions were prompted by a wider variety of work practices, ranging from making decisions about permissions to fielding explicit user requests. As a result, the Android ecosystem featured more diverse and creative privacy solutions.

The contrast between work practices and privacy discussions in iOS and Android suggests that another class of developers—*platform* developers—can serve a powerful

role in encouraging ethical practice within their ecosystems. Firms that host mobile application stores function as centralized distribution points for mobile software. That centralization should prompt these firms to consider their role as regulators, deciding whether they will demand particular privacy-oriented features from applications within their marketplace. Google and Apple are not only hosts of developers' designs, but also (private) regulators of those designs. The different structures of those development environments prompt different moments of ethical deliberation. While they are not content producers, platform firms influence design ethics; as Gillespie (2010) notes, platforms are constantly engaged in ethical, legal, processual, and financial decisions about the content they host. Within mobile development, this opens an opportunity for platforms to potentially structure developer *work practices* to encourage ethical debate, deliberation, and justification. Imposing technical constraints through operating system features, for example, prompts developers to question and debate why those technical constraints exist. This power exists even if developers are not formally employed by Apple or Google, simply because they must use the platform's code and comply with the platform's regulations. Illustrating the wide range of third parties who may have access to personal data can help developers understand the consequences of sharing or selling user data. Giving developers diverse options for data collection permissions, and enabling users to select among those options, helps developers be conscious that users might prefer to limit data collection and access. Linking developers more directly to users through forums or feedback can also increase developers' attention to privacy by making user concerns a part of the development dialogue. And finally, finding ways to encourage developers to differentiate their products based upon data protection features can encourage a marketplace of privacy-sensitive options for consumers.

For educators, regulators, and managers interested in encouraging more ethical discussion and deliberation in mobile development, the values levers in each ecosystem provide a valuable point of entry. Apple's regulation process provides an excellent opportunity for regulators to collaborate with a major industry stakeholder to decide whether and if privacy concerns are being sufficiently addressed by the Apple approval process and the technical constraints that Apple places on development for its operating system. The Android ecosystem's tight integration between users and developers provides an opportunity for users to organize for better privacy protections. Disseminating evidence-based research about user expectations and needs through Android forums might be one way to trigger additional ethical deliberation.

Engaging with analytics provides an opportunity to encourage developers in both ecosystems to be more reflective about the data they collect and store. Managers interested in encouraging ethical discussions might find ways to highlight the many third parties who can access iOS and Android data. And helping developers to see the extent and reach of third parties involved in their ecosystems, from data brokers to advertisers, could also spur additional ethical discussion.

In future work, our team will evaluate a number of these values levers as educational interventions. We are building interactive simulations for use in mobile development classrooms and workshops. These simulations ask teams to define data collection policies for a mobile application. The simulations deploy values levers discovered here by requiring teams to gain App Store approval, navigate technical constraints, decide upon permissions, and get feedback from users. Running different simulations and contrasting the results will allow us to evaluate the efficacy and impact of various values levers.

A final finding of this research is that while the triggers for privacy conversations are quite different between ecosystems, ultimately the justifications offered for privacy are similar. Developers across both ecosystems use moral and cautionary tales, moral evaluation, and instrumental and technical rationalization to legitimize privacy as a value in mobile development. Mimicking all three forms of justification for privacy can be useful to those who wish to promote ethical practices in mobile development—and indeed, each of these forms of justification is likely familiar to ethics researchers and educators. Contributing moral and cautionary tales which are both accurate and meaningful could be a way of increasing ethical dialogues in online forums. And paying attention to the importance of instrumental and technical rationalizations—without losing the overall point that not all ethical principles can be rationalized—can help us to find situations in which a boon for privacy is also a boon for a technical concern (such as power consumption).

A next step for this research is to understand *why* justifications for privacy are so similar. One observation was that while developers from all over the world participated in the forums, the privacy discourses engaged were largely American in tone and outlook. Moral evaluations largely framed privacy was a principle of individual liberty. Rationalizations found market justifications for respecting privacy. And cautionary tales taught developers that privacy violations might result in lawsuits. Largely missing were more stringent European perspectives on data protection (Jones 2016), or even non-western views more focused on communal norms than individual liberties (Capurro 2005). Some of the very American nature of our data is likely explained by the fact that we analyzed

English-language forums (though each forum involved many international participants). We further hypothesize that because Google and Android are both American companies, they shape the discourse of their developers toward American cultural norms. Future research to test this hypothesis is one outcome of this qualitative study.

Our analysis of privacy levers and justifications in mobile application development leaves open several other questions for future work. A re-analysis of the forum data focused on the progression of privacy debates *over time* might be very revealing of when and how privacy standards emerged as these development communities matured. Second, because we searched for threads that explicitly discussed privacy, we have found few examples of application design in which privacy was not considered, or concerns were suppressed or ignored. Methods to find such conversations might involve tracing the historical development of apps which were deemed by consumers or regulators to have significant privacy concerns once they reached the marketplace.

Conclusion: Advancing Ethical Dialogue in Technology Development

Values levers cannot fully solve the challenge of integrating ethical decision making into technical development settings. But particular work practices can advance the dialogue, contributing to a culture of ethical reflection within technical work. Analyzing the relationship between work practices and ethical discussions across two mobile development platforms demonstrates that gaining the approval of a regulator, navigating technical constraints, debating permissions, dealing with requests from users, using analytics, and interacting with third parties can all spark conversations about privacy during mobile development. Discovering these practices points to actors who can be influential in encouraging ethics-oriented software design, including mobile platform companies, analytics companies, and users in addition to ethicists and educators. Articulating these practices, and the ecosystem of firms and individuals who encourage those practices, moves us one step further toward encouraging developers to prioritize privacy practices and features in software design.

Acknowledgements We would like to thank participants at the 2016 iConference and the 2016 Privacy Law Scholars Conference for feedback on early drafts of this work.

Funding This study was funded by the US National Science Foundation Awards CNS-1452854, SES-1449351, and a Google Faculty Research Award.

Compliance with Ethical Standards

Conflict of interest Shilton has received research grants from Google. Google has not approved or influenced the results of this study.

Ethical Approval All procedures performed in studies involving human participants were in accordance with the ethical standards of the institutional research committee and with the 1964 Helsinki Declaration and its later amendments or comparable ethical standards.

References

Ashworth, L., & Free, C. (2006). Marketing dataveillance and digital privacy: Using theories of justice to understand consumers' online privacy concerns. *Journal of Business Ethics, 67*(2), 107–123. doi:10.1007/s10551-006-9007-7.

Balebako, R., Marsh, A., Lin, J., Hong, J., & Cranor, L. F. (2014). The privacy and security behaviors of smartphone app developers. In *USEC'14*. San Diego, CA: Internet Society. Retrieved from http://lorrie.cranor.org/pubs/usec14-app-developers.pdf

Brey, P. A. E. (2012). Anticipating ethical issues in emerging IT. *Ethics and Information Technology, 14*(4), 305–317.

Brusoni, S., & Vaccaro, A. (2016). Ethics Technology and Organizational Innovation. *Journal of Business Ethics*. doi:10.1007/s10551-016-3061-6.

Busch, T. & Shepherd, T. (2014). Doing well by doing good? Normative tensions underlying Twitter's corporate social responsibility ethos. *Convergence: The International Journal of Research into New Media Technologies*, *20*(3): 293–315.

Capurro, R. (2005). Privacy. An intercultural perspective. *Ethics and Information Technology, 7,* 37–47.

Cavoukian, A. (2012). *Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices*. Ontario, Canada: Office of the Privacy Commissioner of Canada. Retrieved from http://www.privacybydesign.ca/index.php/paper/operationalizing-privacy-by-design-a-guide-to-implementing-strong-privacy-practices/

Cetina, K. K., Schatzki, T. R., & von Savigny, E. (Eds.). (2001). *The Practice Turn in Contemporary Theory*. New York: Routledge.

Cohen, J. E. (2012). *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice*. New Haven & London: Yale University Press.

Cranor, L. F. (2006). What do they "indicate?": Evaluating security and privacy indicators. *Interactions*, https://doi.org/10.1145/1125864.1125890

Cravens, A. (2012). *A demographic and business model analysis of today's app developer*. Retrieved March 19, 2013, from http://pro.gigaom.com/2012/09/a-demographic-and-business-model-analysis-of-todays-app-developer/

Davenport, E., & Hall, H. (2002). Organizational knowledge and communities of practice. *Annual Review of Information Science and Technology (ARIST), 36,* 171–227.

Drover, W., Franczak, J., & Beltramini, R. F. (2012). A 30-year historical examination of ethical concerns regarding business ethics: Who's concerned? *Journal of Business Ethics*. doi:10.1007/s10551-012-1214-9.

Federal Trade Commission. (2012). *Protecting consumer privacy in an era of rapid change: recommendations for businesses and policymakers*. Washington, DC: Federal Trade Commission.

Friedman, B., & Nissenbaum, H. (1997). Bias in computer systems. In B. Friedman (Ed.), *Human Values and the Design of Computer Technology* (pp. 21–40). Cambridge and New York: Cambridge University Press.

Froehlich, J., Findlater, L., & Landay, J. (2010). The design of eco-feedback technology. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 1999–2008). New York, NY, USA: ACM. https://doi.org/10.1145/1753326.1753629

Gillespie, T. (2010). The politics of 'platforms'. *New Media & Society, 12*(3), 347–364.

Google Play. (2016). *Google Play Developer Distribution Agreement*. Retrieved August 9, 2016, from https://play.google.com/intl/ALL_us/about/developer-distribution-agreement.html

Greene, D. & Shilton, K. (In press). Platform Privacies: Governance, Collaboration, and the Different Meanings of 'Privacy' in iOS and Android Development. *New Media & Society*.

Gurses, S., & van Hoboken, J. (2017). Privacy after the Agile Turn. In E. Selinger (Ed.), *The Cambridge handbook of consumer privacy*. Cambridge and New York: Cambridge University Press. Retrieved from https://osf.io/27x3q/#

Harris, K. D. (2013). *Privacy on the go: recommendations for the mobile ecosystem*. Sacramento, CA: California Department of Justice.

Herkert, J. (2001). Future directions in engineering ethics research: Microethics, macroethics and the role of professional societies. *Science and Engineering Ethics, 7*(3), 403–414.

Hollander, R. (2009). *Ethics Education and Scientific and Engineering Research: What's Been Learned? What Should Be Done? Summary of a Workshop*. Washington, D.C.: National Academy of Engineering.

Introna, L., & Pouloudi, A. (1999). Privacy in the information age: Stakeholders, interests and values. *Journal of Business Ethics*. doi:10.1023/A:1006151900807.

Jones, M. L. (2016). *Ctrl + Z: The right to be forgotten*. New York; London: NYU Press.

Kelley, P. G., Consolvo, S., Cranor, L. F., Jung, J., Sadeh, N., & Wetherall, D. (2012). A Conundrum of Permissions: Installing Applications on an Android Smartphone. In J. Blyth, S. Dietrich, & L. J. Camp (Eds.), *Financial Cryptography and Data Security* (pp. 68–79). Springer Berlin Heidelberg. Retrieved from http://link.springer.com.proxy-um.researchport.umd.edu/chapter/10.1007/978-3-642-34638-5_6

Kelty, C. M. (2008). *Two Bits: The Cultural Significance of Free Software*. Durham, NC: Duke University Press.

Leon, P. G., Ur, B., Balebako, R., Cranor, L. F., Shay, R., & Wang, Y. (2011). *Why Johnny can't opt out: a usability evaluation of tools to limit online behavioral advertising* (No. CMU-CyLab-11-017). Pittsburgh, PA: Carnegie Mellon University.

Lipner, S. (2004). The trustworthy computing security development lifecycle. In *Proceedings of the 20th Annual Computer Security Applications Conference (ACSAC'04)* (pp. 2–13). Tucson, AZ: IEEE Computer Society. doi:10.1109/CSAC.2004.41

Martin, K. E. (2013). Transaction costs, privacy, and trust: The laudable goals and ultimate failure of notice and choice to respect privacy online. *First Monday*. Retrieved from http://firstmonday.org/ojs/index.php/fm/article/view/4838

Martin, K. E. (2015). Understanding privacy online: Development of a social contract approach to privacy. *Journal of Business Ethics*. doi:10.1007/s10551-015-2565-9.

Martin, K. E., & Shilton, K. (2015). Why experience matters to privacy: How context-based experience moderates consumer privacy expectations for mobile applications. *Journal of the Association for Information Science and Technology*. doi:10.1002/asi.23500.

Martin, K. E., & Shilton, K. (2016). Putting mobile application privacy in context: An empirical study of user privacy expectations for mobile devices. *The Information Society*. doi:10.1080/01972243.2016.1153012.

Miller, J. K., Friedman, B., & Jancke, G. (2007). Value tensions in design: the value sensitive design, development, and appropriation of a corporation's groupware system. In *Proceedings of the 2007 international ACM conference on Supporting group work* (pp. 281–290). Sanibel Island, Florida, USA: ACM. Retrieved from http://portal.acm.org/citation.cfm?id=1316624.1316668

Moor, J. H. (1985). What is computer ethics? *Metaphilosophy*. doi:10.1111/j.1467-9973.1985.tb00173.x.

Mulligan, D. K., Koopman, C., & Doty, N. (2016). Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy. *Philosophical Transactions of the Royal Society A*. doi:10.1098/rsta.2016.0118.

Nissenbaum, H. (2009). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford Law Books.

Nissenbaum, H. (2015). Respecting context to protect privacy: Why meaning matters. *Science and Engineering Ethics*. doi:10.1007/s11948-015-9674-9.

Orlikowski, W. J. (2007). Sociomaterial practices: exploring technology at work. *Organization Studies*. doi:10.1177/0170840607081138.

Pavlou, P. A. (2013). State of the information privacy literature: Where are we now and where should we go? *MIS Quarterly, 35*(4), 977–988.

Shilton, K. (2013). Values levers: Building ethics into design. *Science, Technology & Human Values, 38*(3), 374–397.

Solove, D. J. (2010). *Understanding Privacy*. Massachusetts: Harvard University Press.

Spencer, G. (2016). *Developers: Apple's App Review Needs Big Improvements [Blog]*. Retrieved from https://www.macstories.net/stories/developers-apples-app-review-needs-big-improvements/

Spiekermann, S., & Cranor, L. F. (2009). Engineering Privacy. *IEEE Transactions on Software Engineering, 35*(1), 67–82.

Urban, J. M., Hoofnagle, C. J., & Li, S. (2012). *Mobile Phones and Privacy* (BCLT Research Paper Series). Berkeley, CA: University of California at Berkeley—Center for the Study of Law and Society. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2103405

van Leeuwen, T. (2008). *Discourse and Practice: New Tools for Critical Discourse Analysis (1 edition)*. Oxford; New York: Oxford University Press.

Verbeek, P.-P. (2006). Materializing Morality Design Ethics and Technological Mediation. *Science, Technology & Human Values*. doi:10.1177/0162243905285847.

VisionMobile. (2016). *Mobile Developer Segmentation 2016*. London: VisionMobile.

Waldo, J., Lin, H. S., & Millett, L. I. (2007). *Engaging Privacy and Information Technology in a Digital Age*. Washington, D.C.: The National Academies Press.

Westin, A. F. (1970). *Privacy and Freedom*. New York: Atheneum.

Guston, D. H. (2011). Participating despite questions: Toward a more confident participatory technology assessment. *Science and Engineering Ethics*. doi:10.1007/s11948-011-9314-y.

Zang, J., Dummit, K., Graves, J., Lisker, P., & Sweeney, L. (2015). Who knows what about me? A survey of behind the scenes personal data sharing to third parties by mobile apps. *Journal of Technology Science*. Retrieved from http://jots.pub/a/2015103001/