Bribecaster: Documenting Bribes Through Community Participation

Manas Mittal

Electrical Engineering and Computer Sciences
University of California at Berkeley

Technical Report No. UCB/EECS-2014-85
http://www.eecs.berkeley.edu/Pubs/TechRpts/2014/EECS-2014-85.html

May 16, 2014

Bribecaster: Documenting Bribes Through Community Participation

by Manas Mittal

Research Project

Submitted to the Department of Electrical Engineering and Computer Sciences, University of California at Berkeley, in partial satisfaction of the requirements for the degree of **Master of Science, Plan II**.

Approval for the Report and Comprehensive Examination:

Committee:

Professor Björn Hartmann

Research Advisor

16th May 2014

* * * * * * *

Professor Eric Brewer

Second Reader

16th May 2014

Bribecaster: Documenting Bribes Through Community Participation

Manas Mittal

Computer Science Division
University of California, Berkeley
mittal@cs.berkeley.edu

ABSTRACT

Corruption is endemic in emerging economies – many transactions of private citizens with government institutions require the payment of bribes. While well known as a general phenomenon, specific data about the "bribe economy" is hard to come by. But such data is needed for rational responses to corruption at the societal and individual level – to expose it; to know which offices to avoid; or to know how much to pay if other recourse is not available. In response to a corruption survey of 102 participants, we have developed Bribecaster, a web application and an Android app to enable citizens to report and consume corruption information about dealing with government offices. Bribecaster uses a novel privacy-preserving implicit login schema and one-way hashing for protecting user identities while simultaneously ensuring the accuracy and integrity of reports. This citizen-induced transparency facilitates rational social and individual responses to corruption. Participants in a first-use user study rated Bribecaster highly for its usefulness.

Author Keywords

Privacy, Crowdsourcing, Mobile Applications, Corruption

ACM Classification Keywords

H5.m. Information interfaces and presentation, K.4.1 Public Policy Issues, J.4 Social And Behavioral Sciences

General Terms

Human Factors, Design, Economics

INTRODUCTION

The goal of my research is to learn how to build systems that can foster trustworthy knowledge exchange between anonymous users in sensitive situations. In pursuit of this objective, we have developed Bribecaster – an application specifically designed to anonymously and publically shares sensitive information about the bribe economy in the developing world. Bribecaster also provides a platform to run studies to investigate issues of trust and anonymity.

A significant percentage of the world's population lives in developing countries and corruption is a major problem in many such countries. For example, India has made fighting corruption a key component of its development strategy [1].

Corruption is a two-sided problem. People in positions of power demand bribes for performing or expediting work. Individuals and corporations pay these bribes, which are often considered part of normal business practices in the developing world [1, 2]. Petty corruption frequently involves paying bribes to low and mid-level officials, e.g., in law enforcement, government offices, or to tax and license inspectors [1].

Many efforts to stem corruption focus on punitive action against corrupt officials. This top-down approach is not successful in most developing countries [3]. Could a bottom-up approach—where citizens exchange corruption information with each other—be more effective? To motivate our research, we conducted a formative corruption survey of 102 Indian participants; results indicate that individuals who have had to

pay bribes are open to reporting corruption information. Our research investigates whether bribe market transparency can be achieved by a confidential bribe-reporting application.

We have developed Bribecaster, an application that enables community members to: a) anonymously report their interactions with government functionaries, and b) search existing bribe reports – indexed and segmented by departments, offices and common services provided by an office. Importantly, the application places special emphasis on preserving the anonymity of the reporters while still discouraging malicious reviewers.

Reporting bribes has two principal benefits: first, disseminating information about the bribe market can empower individuals to make rational choices, for example, deciding to seek out a different office, or deciding how much to pay [4]. Secondly, transparency can draw public attention to violations. Such scrutiny may ultimately lead to a decrease in corruption levels. We are initially targeting India, because of our team's experience, India's significant English speaking population, and its democratic government, which should be receptive to anti-corruption measures [5].

Harassment Bribes

Bribes are sometimes paid in exchange for receiving undue favors from public officials, such as getting government contracts. Frequently however, bribes have to be paid to receive a service that the citizen is otherwise entitled to. For example, getting a tax refund often involves paying a part of the refund as a kickback. Such bribes are called *harassment bribes* [6]. While the government functionary cannot legally deny services, they can aggravate delivery or delay the service. Harassment bribes raise the effective price of public goods and services, reduce trust in good governance, often serve as a regressive tax, and prevent access to basic services [7]. We are specifically interested in collecting information about harassment bribes.

Asymmetric Liability

The current legal framework in most countries makes it illegal to both pay and accept bribes. Basu et al. [6] have suggested that this leads to a convergence of interests between the bribe payer and the bribe taker. They advocate introducing asymmetric liability – a mechanism where bribe-takers are culpable but bribe-givers have legal immunity. This divergence of interests will lead to a better "mutual check"—officials are less likely to demand bribes when the payer has no incentive not to report it.

While such political and legal change is being suggested by government economists, it is unlikely to be implemented given the historical lack of political will to affect such change. Additionally, politicians may be part of the corruption chain where slices of bribes collected by lower officials are passed up the government hierarchy, all the way to the top elected officials. By enabling individuals to report their bribe experiences anonymously and publically, Bribecaster provides an informal alternative to legislative changes needed to install asymmetric liability. This introduces a key challenge in the design of the Bribecaster system – protecting the reporters' privacy. This objective trumps all others.

BACKGROUND

In order to evaluate the utility and feasibility of Bribecaster before building the system, and to inform our design, we deployed a formative survey (Appendix 1, 2) [8]. The survey enabled us to gain insight about the prevalence of corruption in India, the willingness to report and share information about it, and the current technology environment. The survey was deployed on Amazon Mechanical Turk, which has a large Indian workforce. We collected 102 responses over two days, and paid each participant $0.25. Our results have a potential bias in that respondents may be more tech-savvy than the general population. However, we have no reason to believe that participants will show a systematic bias in reporting corruption behavior.

The key findings of the survey were:

Most Respondents Pay Bribes

90% (92/102) of respondents indicated that they had given bribes in the past, and over 82%

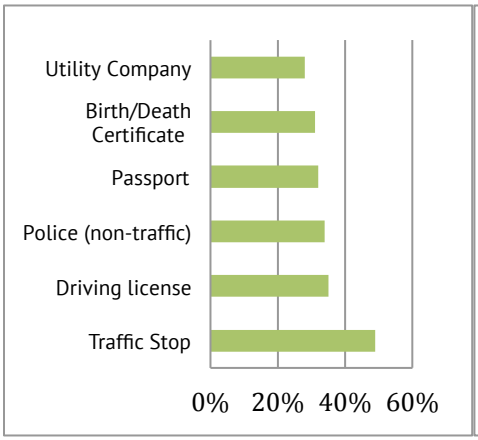


Fig. 1: Common transactions that required payment of bribes

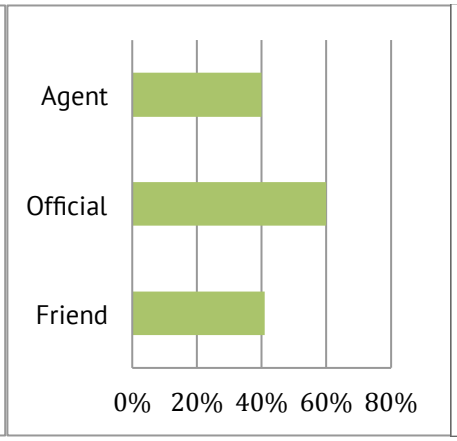


Fig. 2: Common sources that provided information about bribe prices

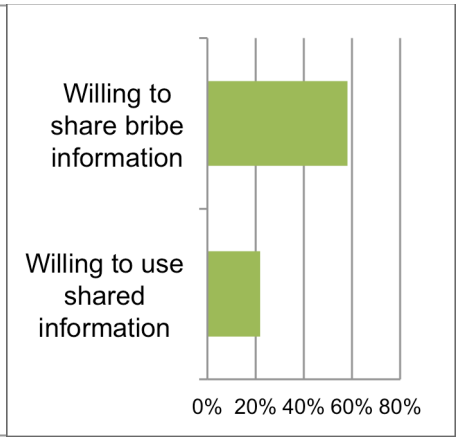


Fig. 3: Respondents are wary of shared information

(84/102) identified specific individuals to whom they had paid bribes. Fig. 1 shows transactions that often required bribes. These responses indicate that corruption is pervasive and that harassment bribes are common– for example over 30% of respondents paid bribes to get a passport.

Respondents Use Outside Information to Price Bribes

We asked participants about how they determined the price to pay for a bribe: 60% (56/92) of those who paid a bribe indicated the official provided a number; 41% indicated that their friends told them the amount, and 40% indicated that a middleman (commonly referred to as an "agent") told them the appropriate amount (Fig. 2). Agents are valuable because they know who to bribe and how much to pay. Such information could also be obtained through a crowdsourced database of bribe reports, and provides an important incentive to consume information from a system like Bribecaster.

Respondents Already Share Their Bribe Experiences

We next asked about existing forms of bribe-related information exchange: 52% had told friends or relatives about paying bribes because they felt bad about the transaction; 34% told others to keep them informed. Only 14% did not report paying a bribe because they felt embarrassed. The high level of informal sharing, and the low level of embarrassment about paying bribes suggest that users may be willing to share information electronically.

Respondents Are Wary of Anonymous Information

When explicitly asked if subjects would anonymously report bribes through a website or mobile application, 58% responded positively. Would respondents use anonymous bribe information? Fig. 3 shows that of those who had valid answers, 22% indicated yes, while 78% indicated no. More people are willing to report bribes than are willing to use this information. We speculate that this result may be due to a lack of trust in anonymous reporting. We conclude that the trade-off between trust and anonymity is a key design consideration.

RELATED WORK

There are both commercial applications and academic research on corruption. IPaidABribe.com [4] is a website for collecting bribe-related citizen reports, and Bribespot [9] is an iPhone app with similar functionality. Both these applications are focused on reporting bribes, but do not provide specific bribe information, thus diminishing their usefulness. In contrast, Bribecaster records and provides fine-grained actionable information. Additionally, both Bribespot and IPaidABribe.com do not address the tension between anonymity and trust.

While IPaidABribe.com has a similar reporting structure to the Bribecaster interface, it has different objectives, mechanisms and philosophy. IPaidABribe provides no explicit anonymity guarantees to bribe reporters. Instead, its privacy policy states that it will willingly provide information to state actors and law enforcement, potentially jeopardizing the bribe reporter's safety. The site then deals with the apparent illegality of such reports by rendering them toothless – official names and offices are (perhaps manually) redacted from the reports. It appears that the intention is to "not ruffle the feathers" and is thus bound to remain largely ineffectual in affecting change. In contrast, Bribecaster attempts to protect the reviewers by anonymizing their identities, but retains the names of people and offices mentioned in the review, and incorporates mechanisms to thwart malicious actors.

Review Systems

Review websites rely on users to write reviews. Malicious users may write fake reviews to promote or demote a target entity. In practice, such false reviews are widespread [10]. Techniques to detect such reviews often rely on examining the behavior for a given user account [10]. This is not possible in situations where a user is anonymous and there is no history of past behavior available for a particular user.

Prior research has focused on creating trust in decentralized anonymity networks [11], but our problem of having a centralized server and a web-based user interface is not addressed. Yelp.com uses a filter [12, 13] to display only the most trusted reviews, but their algorithm relies on the existence of trusted users—something that we cannot use in an anonymous system.

Establishing Identity Anonymously

Bribecaster must prevent malicious users from filing multiple reports and skewing results in a particular direction.

Keystroke dynamics [14, 15] identifies and authenticates users based on their typing patterns. The user's keystroke rhythms are measured and recorded. A unique biometric signature is then developed for each user. Keystroke dynamics, while interesting, is not particularly suited for the users of Bribecaster. Bribecaster users are likely to be in-experienced and infrequent keyboard users. Such users display typing patterns with a high variance. It is technically difficult to establish a typing biometric in such scenarios [16]. Therefore, we do not currently incorporate keystroke dynamics as part of the user's implicit identity signature, but use alternative mechanisms (described later) for establishing such identity.

THE DESIGN OF BRIBECASTER

We now explain and discuss our design rationales for the Bribecaster web application.

The Bribecaster web application allows users to search for and report transactions. The front-page (Fig. 4) shows recent bribes in an updating stream and map display, and provides both search and reporting forms.

The reporting form (Fig. 5) asks for:

1) Amount of the bribe if any (Fig. 5–1)

2) Name or title of official (Fig. 5–2)

3) Activity / task (Fig. 5–3)

4) Department name (Fig. 5–4)

5) Office address or location (Fig. 5–5)

6) An extended comment (Fig 5–6)

Fig. 4: The front page shows a feed of new bribes, our anonymity policy, and a streamlined reporting form. (1) Search box for the type of activity, with autocomplete (2) Name of the city of vicinity, defaults to city based on user's IP and autocompletes (3) Reporting form for a Bribe report, the activity, department and location fields autocomplete. (4) Newsfeed indicating a recent bribe (5) Newsfeed bribe location (6) Privacy Policy

The location and transaction fields support autocomplete. The location field's autocomplete suggests nearby offices or previously entered entities. The list of nearby office is provided by the Google Places API [16]. This API requires the latitude and longitude to center its search around. This is determined based on the user's IP address, and then using an IP to City Name mapping database (PyGeoIP [17]). The task Autocomplete suggests previously entered transactions. Similar autocomplete functionality is provided throughout the Bribecaster service (Figs. 5, 6, 9). The autocomplete feature facilitates the easy entry of structured text information. Additionally, it promotes the user-reconciliation of duplicate offices & tasks at the time of text entry.

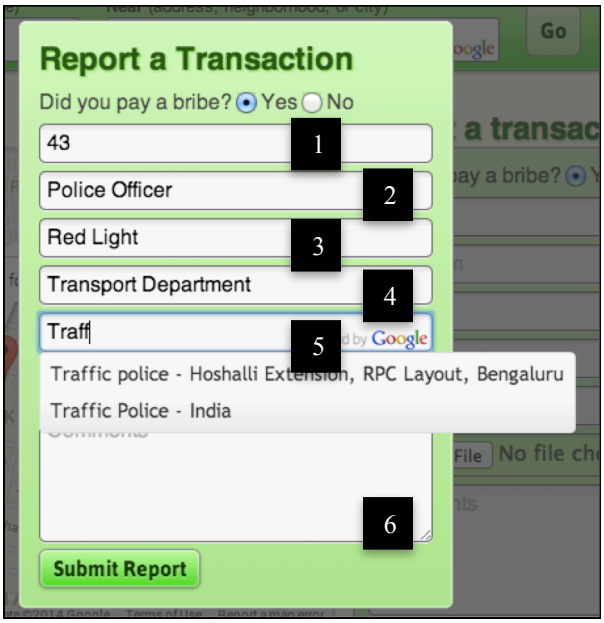


Fig. 5: Autocomplete for bribe reporting input (Field 5 Autocomplete suggests nearby offices)

Fig. 6: Autocompleting based on office locations in a given city. Default city is selected based on the user's IP location.

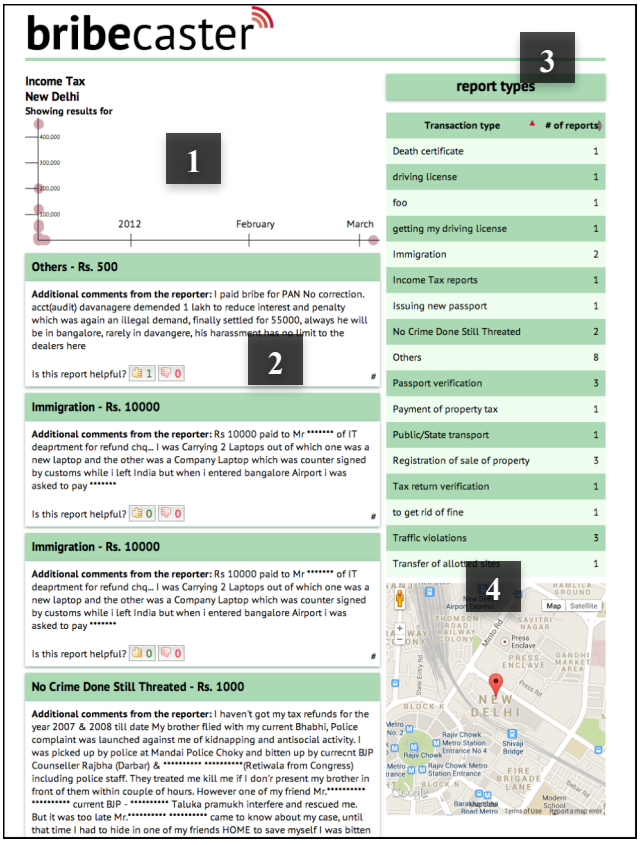


Fig. 7: Reports for a given office (Income Tax, New Delhi). (1)Time series graph of reported bribes, (2) bribe reports for the office., thumbs up/down button (3) Segmented by tasks performed at a given office, (4) Office location

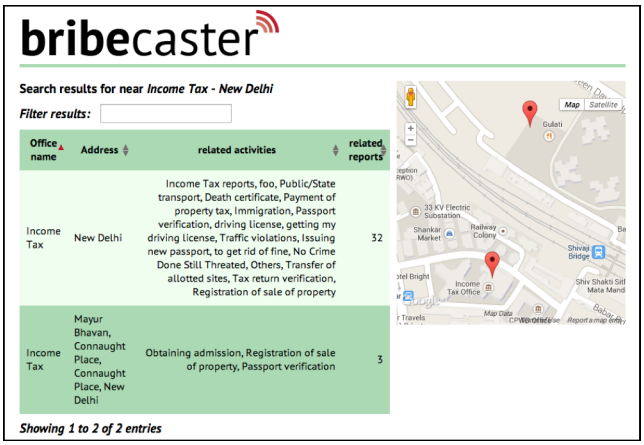


Fig. 8: List of Reports within a given office (Income Tax Department, Delhi) when the task field is left blank. This identifies two offices – one in New Delhi, and another in Mayur Bhavan, Cannaught Place, New Delhi.

Users are therefore less likely to erroneously create new misspelled entities.

Search is the primary navigation mechanism provided by the Bribecaster system. Users can search for bribes based on a specific location that defaults to their current location.

Each office has its own page (Fig. 7). All the corresponding transactions are shown, or they can be filtered by keywords. The top of the page features an interactive graph (Fig. 7–1) built with d3.js [18] that shows how bribe amounts for transactions have changed over time. Selecting a report type in the right column filters the transactions and the corresponding graph to only those that match the selected type.

A key construct of Bribecaster is to rely on users to provide signals for other users about the veracity and usability of the reports. Reports can be marked as thumbs up or thumbs down (Fig 7-2) by readers, signaling the usefulness and reliability of the report. Location pages, including those with keyword filters, have human-readable permalinks for easy sharing. Individual transactions have dedicated pages as well. Location pages also contain a direct link to report additional transactions at that location (Fig. 8). By restricting our system to just a few easy-to-understand page types, we hope to have a cohesive and streamlined user experience.

Fig. 9: List of tasks at a given office (Optional)

ANDROID APPLICATION

We have also developed a Bribecaster Android application. The Android application employs the same backend cloud services that are used by the web application. The remainder of this section discusses the Android user interface. Figs. 10 – 17 present snapshots of the UI.

Reporting Interface

The Bribecaster Android application allows users to enter and browse bribe reports (Fig. 10). The input form lets reporters indicate if they had to pay a bribe (Fig. 11) or not (Fig. 12). The 'What' field tries to autocomplete based on popular reports from the user's current location, but is not restricted to previously reported activities. Touching on the 'location' field brings up a list of nearby locations that have either been previously indicated by other reports, or were gleaned from the Google location APIs (Fig. 14). The user can also add a new location (Fig. 13) thereby adding to the list of known offices our database.

Search Interface

The bribe display interface is shown in Figs. 15 – 17. The map (Fig. 15) defaults to nearby offices for which reports are available, and the user may choose a given location and see a list of reported bribes in a specified area. The user is then shown titles of the bribe reports for that office and key amounts (Fig. 17).

Fig. 10: Android home screen

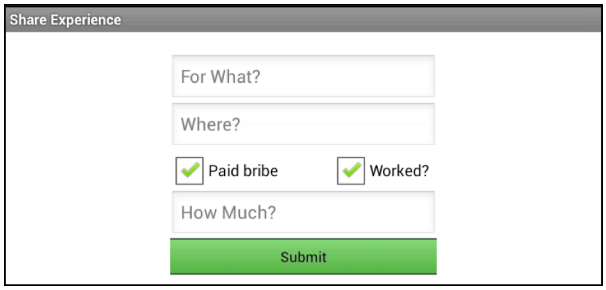


Fig. 11: If the user chooses 'Paid Bribe,

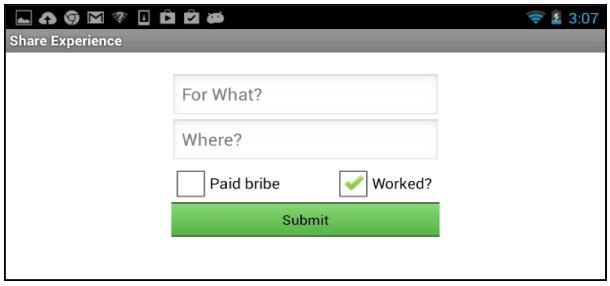


Figure 12: Share experience default page.

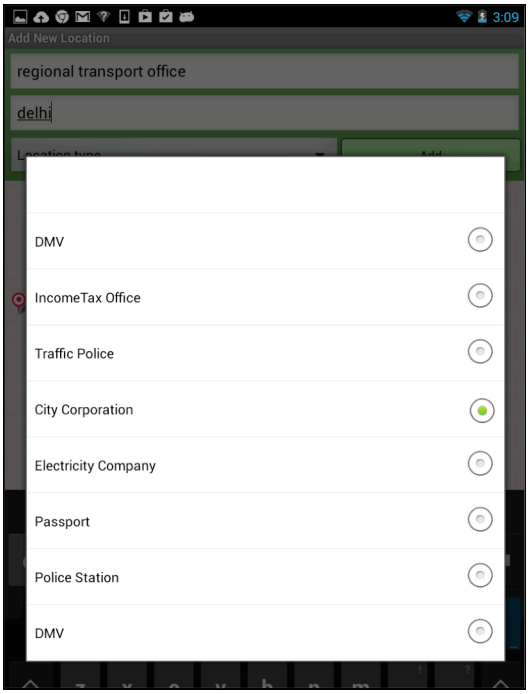


Fig. 13:Adding a new location to the list of reportable locations

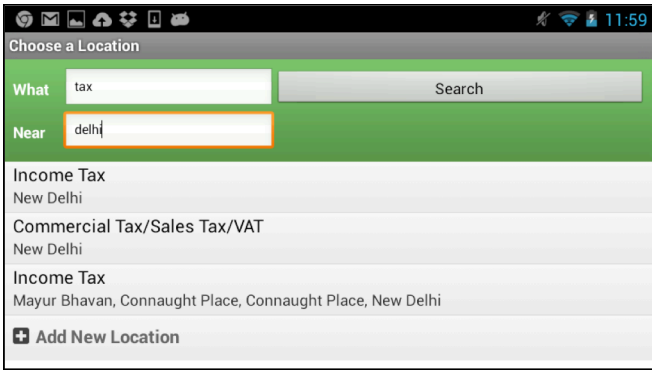


Fig. 14: Share experience location default page

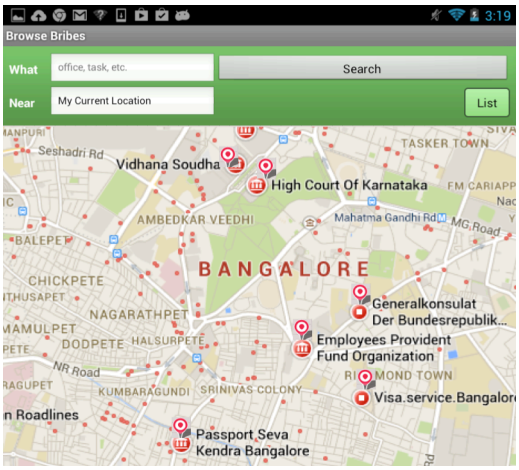


Fig. 15: Browsing bribes. Marks indicate locations for which bribe reports exist.

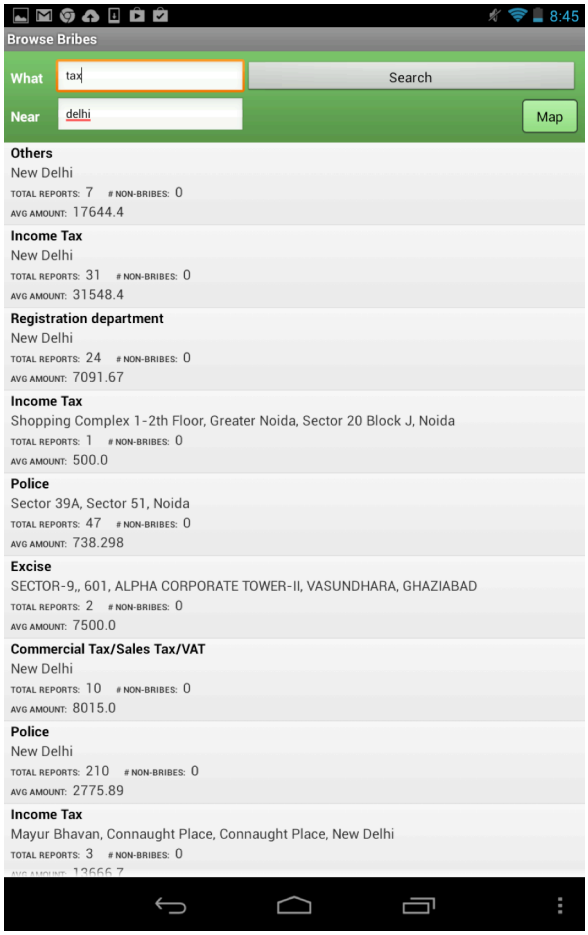


Fig. 16: Browsing a textual list of offices corresponding to searching for 'tax', near 'Delhi'

Alternatively, users can search for a task an office, or a combination thereof. For example: searching for 'tax' near 'Delhi' lists departments where reviewers have used the word 'tax' to describe the task they have performed at the office, and where the office is within or near Delhi (Fig. 16). The user can then choose a specific office of interest and see individual bribe reports (Fig. 17). A user may also see all tasks and individual reports for a nearby office.

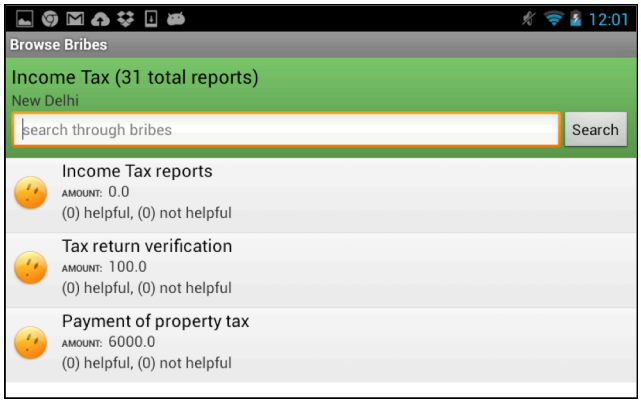


Fig. 17: Browsing details for a given bribe

IMPLEMENTATION

Scalability & Modularity

Bribecaster is built on the Python web framework web.py and runs on Amazon EC2. Bribecaster has the potential to go viral, so the scalability provided by EC2 is vital to our implementation. The EC2 server handles the back-end and maintains the database. At the moment there are two application front-ends that access this server: an Android app and a web application, which we used for our studies. The modularity provided by this server makes it straightforward to extend Bribecaster to new web-enabled platforms. Fig. 18 shows our system architecture. Additionally, the EC2 servers are based in the United States, and provide a certain level of physical security.

Data Model & Search

Bribecaster uses a MySQL database with Python SQLAlchemy wrappers to provide an object relational mapping for our data. Our data model has two classes of objects – the transaction class and the office class. The transaction class covers both bribes and bribe-free dealings. The office class includes an indexed location. A many-to-one relationship maps transactions to offices. Using IP geolocation and the Google Places API, we allow users to search for offices in their proximity. When transactions are added, their locations are added to our database if they are not yet present. This method uses Google Places to supplement location search, but does not rely on it completely because we maintain a local database of locations.

The Bribecaster server features a search provider to efficiently search for transactions near locations. Built on top of the SQLAlchemy ORM, our search provider returns bribe transactions at locations within a given radius of GPS coordinates provided by IP geolocation or by city-based geolookup. It also facilitates autocomplete for locations in both searching and reporting, which improves the user experience.

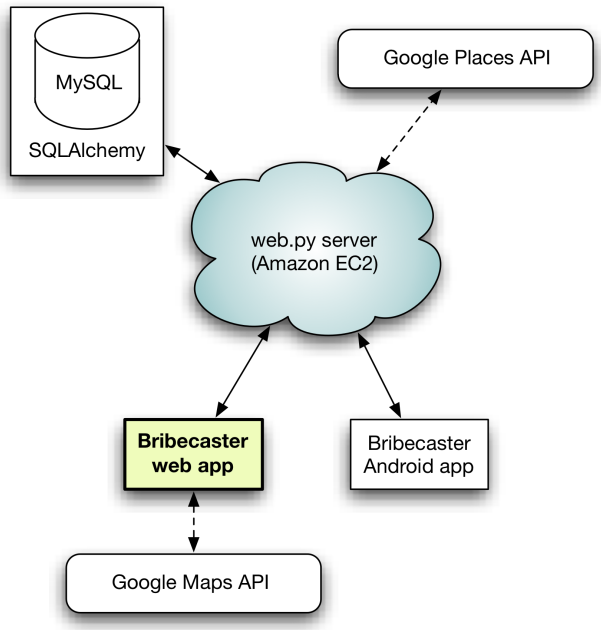


Fig. 18: Bribecaster architecture

USER PRIVACY & MALICIOUS BEHAVIOR

We have implemented multiple privacy protection mechanisms to preserve the anonymity of our users. Users who visit the web application are not tracked using conventional methods like cookies and logins, which are potentially incriminating indicators of participation. While we do not expect repercussions for users who merely browse the site, we hope to protect those who submit sensitive information. Instead, a submitted transaction report is indexed using a salted one-way hash of the submitter's IP address, which then serves as an "implicit login" on behalf of the user. The salted one-way hash is computed by, first taking the user's IP address and 'salting it' by appending a randomly generated string. This string (*salt*) is also stored locally in the database. A SHA-2 cryptographic hash function (SHA-512) is then used to compute a one-way hash of this salted address.

Note that using this technique makes it extremely onerous for any individual (including the site administrators) to decode a submitter's IP address, although a brute force decoding attack is still possible. The brute force attack can be

orchestrated by obtaining access to our database and then searching through the IP namespace. Note that such an attack is likely to be beyond the scope of an individual and would require considerable technical and legal governmental resources.

Malicious users may attempt to attack Bribecaster in several ways. A common scenario in review systems is a user submitting one or more false reports to skew the overall ratings for an entity. For example, a malicious reporter may post a number of fabricated reviews to falsely boost or degrade the reputation of an office. To thwart such behavior, we identify multiple reports from the same IP address, and flag such reports for manual review. The manual review process uses features like the time of reports, the language similarity, and the diversity of reviews from a given IP as a signal to express the level of confidence about the authenticity of a given review. We currently display the text of a low-confidence review but do not use it to compute the integrity score for an office.

This approach provides a first level check against malicious activity. However, it has its shortcomings and is susceptible to false positive and false negative identifications. First, an IP address may be dynamically allocated and can change every time a user re-connects to the Internet. This user would not be identified as an existing user (false negative). Second, a cyber café may have a persistent Internet connection wherein such an IP address does not change, but is likely to be used by multiple users (false positive). Third, we found that users might occasionally use an Internet proxy to display an alternative IP address as their source. Multiple users may use the same Internet proxy (false positive) or a single user may use multiple Internet proxies (false negative). In the future, we may incorporate textual analysis techniques to identify such reviews.

We also have SSL enabled on the site to protect against *man in the middle* attacks. These attacks might be orchestrated by ISPs on behalf of the local law enforcement.

Android phones often hop across multiple IP addresses, and we employ alternative techniques for them. Android phones have a unique ID. We record the salted one-way hash of this unique ID to implicitly identify a user. When reporting a bribe, a user can opt to disclose their location to the Bribecaster app. Such reports are automatically added to the database and available for general display. Non-location verifiable reports are manually screened and approved.

Android phones provide multiple unique identifiers that can be used to identify the phone or the SIM card. We currently use the SIM card signature to identify a user. This is based on our experiences in the developing world where phones are often recycled, but SIM cards are linked to the phone number and are retained by the original subscriber. If a user files multiple reviews for the same office and the same task, within a single month time window, we flag such reviews for manual screening prior to acceptance. We will refine our manual screening heuristics as we gather more data including suspect reports. We also considered explicitly indicating to the user that such multiple reviews will be rejected. However, we rejected the idea - explicitly calling out the user may suggest to them that they are being tracked. Additionally, we hope to protect against the scenario wherein a user's phone is appropriated by a corrupt official attempting to determine if the phone had been used to file bribe reports.

EVALUATION

We evaluated Bribecaster along several different dimensions: usability, usefulness, trustworthiness, virality, and the ability to thwart malicious reporters. These experiments were performed on the Bribecaster web UI. The Android UI was not evaluated.

Our test participants were Amazon Mechanical Turk [19, 20] workers from India. As evidenced by our formative survey, these participants are likely to have had paid bribes in the past. Although a longitudinal study conducted over a few years would have been ideal, Mechanical

Turk workers were a good proxy of early-adopters of Bribecaster.

Mechanical Turk workers were asked to report a randomly generated code that was provided on the Bribecaster webpage. This code was mapped to the users IP address and enabled us to match participants across Bribecaster and Mechanical Turk.

Exp. 1: User Interest & Engagement

To evaluate the usability and utility of Bribecaster, we recruited 122 participants. We wanted to explore if participants would find Bribecaster interesting and engaging?

Participants: We recruited 122 Mechanical Turk workers, paying them $0.10 to perform the given task.

Task: We prepopulated the site with reviews that were scraped from iPaidABribe.com [4]. We asked the user to visit the Bribecaster website, and explore it. We suggested that he/she explore the site by searching for up to five bribes, and/or by browsing the bribe reports and/or reports from the recent bribe feed. We intentionally underspecified the task. We clarified that we will pay the user for merely visiting the website.

Results: We tracked the general level of engagement of the users in a free form searching and browsing task (n=122). We prompted participants to perform five searches or fewer, but on average, participants performed over six searches suggesting that participants were highly interested and engaged. Fig. 19 shows a histogram of the number of searches performed. Additionally, across all our studies, the average participant (n=122) spent 8.25 minutes on the website. Again, this is quite high. Our bounce rate was about 28.22% and participants visited 9.06 pages on average.

Overall, study participants were enthusiastic about Bribecaster and suggested many qualitative improvements and new ideas. Several participants commented that the website was very useful. One offered to reach out to the local media on our behalf to popularize the website. Participants also

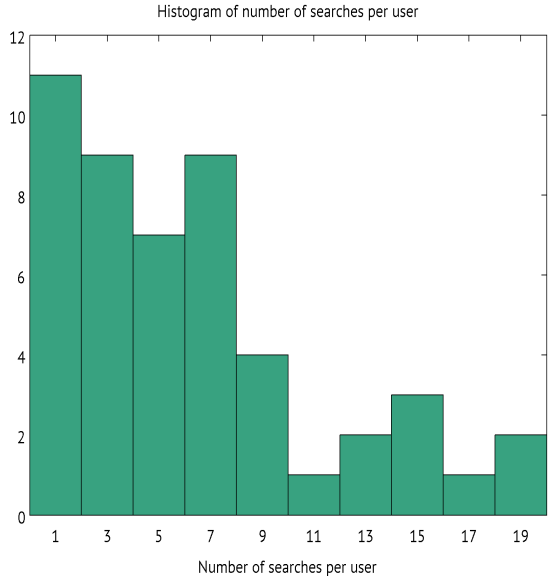


Fig.19: Users in the free form tasks searched more than we asked them to.

gave design suggestions—one proposed improving the design of the website to make it look more professional. He believed that this would make the site more credible, while others suggested changes to format and layout.

Exp. 2: Safe to Report & Trust

In another experiment, we wanted to evaluate if the participants felt safe and whether they trusted the anonymity preserving mechanisms of Bribecaster.

Participants: We recruited 19 India based Mechanical Turk workers.

Task: The task was identical to Exp. 1. Participants were then asked to answer a post-task Likert style questionnaire (Appendix 3). We collected 19 valid responses (Appendix 4).

Result 1 - Participants felt safe: Participants felt safe and anonymous when using Bribecaster (μ=3.89, σ=1.24 where 1= not safe & anon., 5 = very safe and anon.). Most participants felt safe to report the names of specific officials on Bribecaster (μ=3.89, σ=0.93 where 1= not safe and 5 = very safe). Unrelated to Bribecaster, participants (16/19) expressed that privacy was a big concerns when reporting corruption information.

Result 2 - Participants trusted reviews: After inviting participants to search and explore these reviews, 10/19 participants stated that they felt comfortable relying on information that others have submitted. (μ=3.8, σ=1.01 where 1=not comfortable, 5= very comfortable).

Exp. 3: Virality, and Net Promoter Score

The success of a two-sided market such as Bribecaster depends on its adoption by a critical mass of people. A high *virality factor*, i.e., the willingness of users to recommend the system to other users, is critical to the future success of Bribecaster.

Net Promoter Score (NPS): We use NPS [21] as a primary metric to gauge the virality of the system. NPS also serves as a proxy for user satisfaction. The NPS is calculated by asking the following question:

*On the scale, 0: not at all likely, to 10: extremely likely: "*How likely are you to recommend Bribecaster to a friend, colleague, or relative?"

NPS is defined as the number of nines and tens minus the number of zero to six responses. We use NPS as a success metric while we continue to develop and tweak the system. In Fig. 8 we plot the NPS against different versions of Bribecaster with various features enabled.

NPS is an important virality metric. However, in our case, participants were recruited from Mechanical Turk and paid for participating in our studies, and may be positively biased, i.e. they may believe that we would prefer one responses over others and skew their responses to match our (perceived) preferences. However, we did notice relative variations among the net promoter scores. For example, participants in the study who were asked to enter multiple reports maliciously, and failed, showed a higher NPS (NPS = 30) than in other tests. This suggests that the relative NPSs serves as a useful indicator despite potential biases. In general, our NPS scores trended upward and helped us refine our design.

Result: The overall NPS was 23.49 with number of participants = 100.

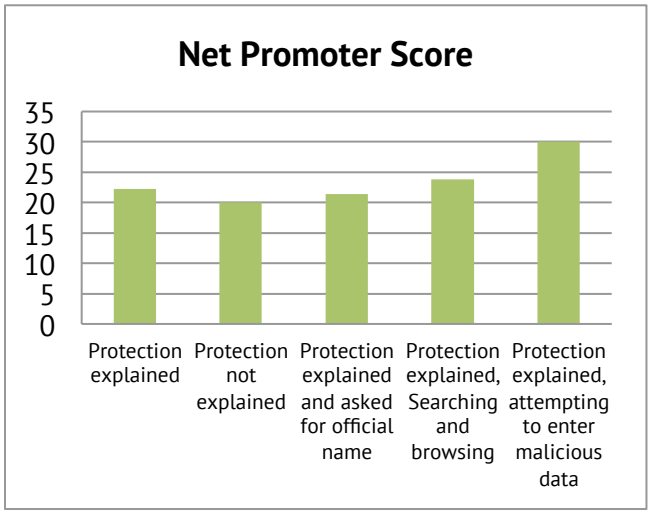


Fig. 20: The change in Net Promoter Score over time, as features are added and removed

Exp. 4: A/B Tests to Select Features

We ran A/B tests [22] with five variants of Bribecaster. The first three variants differed in the messaging of the privacy protection mechanisms. Two other variants required the participant to perform different tasks.

Participants; We recruited 100 participants from Mechanical Turk, with a prompt and setup similar to Experiment 1.

Experiment Design: We divided the 100 participants into five cohorts of 20 participants each. Each cohort was exposed to a different version of Bribecaster, or asked to perform different tasks.

Cohort 1: Privacy protection mechanisms were briefly explained.

Cohort 2: Privacy protection mechanisms were not explained.

Cohort 3: Privacy protection mechanisms were explained, and the participant was asked to enter a report that included the name of the corrupt official.

Cohort 4: Privacy protection mechanisms were explained, and the participant was asked to search and browse results.

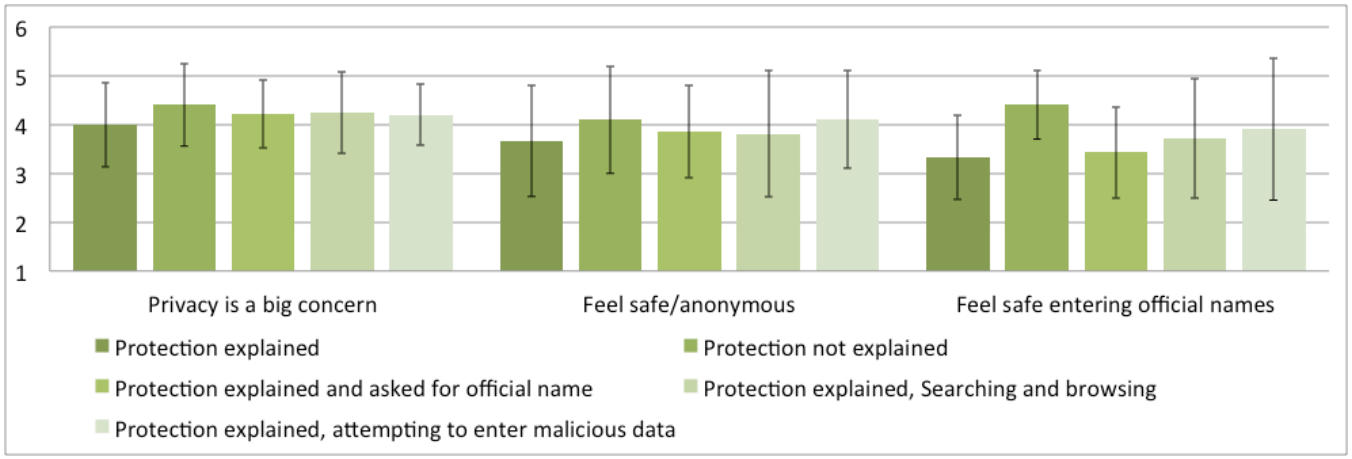


Fig. 21: Results of A/B tests on Mechanical Turk that test how users react to different features of the site. These charts show the mean and standard deviations of responses on a Likert scale (1- strongly disagree, 5 – strongly agree)

Cohort 5: Privacy mechanisms were explained, and the participant was asked to try and enter multiple reports for the same office (simulate a malicious actor).

Fig. 20 displays the different NPSs based on these feature cohorts. Fig. 21 indicates that users of cohort 5 were the most enthusiastic about Bribecaster. We speculate that this may be because participants found the system to be robust against simple attacks. An alternative explanation could be that such participants were most invested in Bribecaster, having spent more time devising strategies to enter multiple reports.

Results: Fig. 21 shows the Likert scale responses for the five cohorts. One surprise was that participants from the cohort where no mention was made of any privacy protection features felt safest when asked to entered official's names (μ=4.4).

Exp. 5: Preventing Multiple Reviews

As usage increases, Bribecaster may attract malicious users. The key attack we have to guard against is when one or more users file multiple false reviews to malign or embellish the reputation of a individual or an office. Our key strategy is to limit the number of reports that an individual (or set of conspiring individuals) can file.

An ideal system would enforce a "*One Person, One Vote*" policy. We evaluated the efficacy of an approach that restricted the numbers of reports from a given IP address to achieve this ideal.

Experiment Design: In a task posted on Amazon Mechanical Turk, we asked participants to post multiple bribes for the same task and office. Participants were prompted to use *any means necessary*. We explicitly stated that users would be paid for successfully reporting a given bribe instance, and not penalized for using any potential mechanism. We encouraged them to be innovative in finding successful approaches. We paid participants $0.25 for attempting the task, and offered a bonus ($0.50) for each multiple report they filed (up to 6 bribes worth $3).

Results: Only one out of ten participants, succeeded in inserting multiple bribe reports. The remaining nine participants spent a median of 8.2 minutes (with some users spending as much as 18 minutes) but did not succeed. The one participant who succeeded inserted three reviews reported using an online proxy (Ultrasurf.com).

This indicates that while the system is beatable, the typical user is unlikely to be able to easily circumvent our present defenses. We also note that our participants were sourced from Mechanical Turk, and are likely more technically competent than the typical user—for example, over 54% of them used the (non default) Chrome browser.

We will continue to monitor and institute additional defenses as the threat model evolves. One approach would involve restricting reports to the same province as where the office is located (based on the reporting IPs), and to blacklist proxy IP addresses.

FUTURE WORK

Study of Efficacy of Intervention

In collaboration with Professors Jennifer Bussell and Thad Dunning (UC Berkeley Political Science & Public Policy), we intend to study the effect of a large-scale Bribecaster deployment on the corruption economy of a region.

"We hypothesize that improving flows of information about the honesty of bureaucrats will influence the usage by citizens of specific offices and reduce the propensity of bureaucrats to ask for bribes." [23]

Bribecaster will present office specific integrity scores similar to the restaurant scores provided by Yelp[13]. These scores will be based on user reports from Bribecaster.

We will then conduct a randomized control trial, wherein a randomly selected subset of bureaucrats is informed of their office's score. We will then use citizen surveys to assess the impact of this intervention on the quality of service delivered and the extent of bribe taking. We will also evaluate the impact of providing citizens with Bribecaster integrity scores via a mobile app, as well as SMS messaging.

Bribecaster as an Information Source

We intend to provide the name and contact information of bureaucrats in charge of each particular office. We will also supply information about the chain of command, and provide a public mechanism to enable users to contact these officials. Additionally, such features will have the added benefit of attracting initial users before a critical mass of user reviews have been collected.

Further, given enough data, we will be able to detect the change in bribe levels as a new official is transferred into or out-of a job. By creating a public 'integrity index' of bureaucrats, we hope to discourage bribe taking.

A Positive System

Bribecaster is currently focused on reporting situations where bribes were demanded and paid. It has a negative skew in that it collects reports of corruption in day-to-day life. Because of this negativity, questions of security and trust are important to consider. In order to skirt these issues, we could re-imagine the system as a primarily positive site, a sort of "Linked-In" for public officials. Users could leave reports of positive transactions and write brief notes of recommendation for officials. If an official had no recommendations on the site, a user could assume that the official was corrupt or in some way untrustworthy. None of the information in this system would need to be private or protected because there is no negative information shared, and it might put pressure on officials to clean up their acts and collect positive reviews.

A Wider Net

One study participant reported a bribe that he had to pay to the functionaries at a private educational institution. Others report having to pay bribes in similar non-governmental contexts. We intend to extend Bribecaster to cover private organizations. We also intend to deploy Bribecaster for other developing regions, particularly Pakistan and parts of Africa. We have also been approached by a Mexico based NGO to deploy Bribecaster there.

Quality Control

Since we do not have a large user base at the time of writing, we have yet to run into issues of quality control. However, if the application becomes popular and receives an influx of transaction reports, we will need to filter out "bad" responses. While typical collaborative applications would use a login system to achieve quality standards, the sensitive nature of our information prevents that. As we gain a better understanding of the abuse patterns, we will develop heuristics and incorporate them into the model, thus decreasing the amount of manual screening needed over time.

Signaling Review Utility

In the future, we will test how upvotes and downvotes of bribe reports, and offices, affect readers. Will users feel more trusting of reviews that have been upvoted? We test this by informing bribe-reporters and viewers that the average bribe report gets four positive reviews. After this, we can measure traffic to particular bribe pages as a metric of interest. Surveys can then be used to determine how people interpret the rankings.

Corruption Index

Widespread use of Bribecaster could give rise to social incentives for administrators and professionals to reduce the level of corruption. One idea is to induce an atmosphere of an informal competition among offices and bureaucrats by periodically publishing an office-specific corruption index.

Increasing Reach

We hope to introduce the following improvements to make Bribecaster more widely available

1. Local language support: In addition to English, Bribecaster will be extended to support local languages, starting with Hindi.

2. Interactive Voice Response System (IVRS): Users will be able to obtain information by calling in and navigating a phone tree. The information provided will be limited to the integrity score for a given office. Users will also be able to submit a report by calling in and recording the details.

3. An improved Android application: The Bribecaster's mobile app will be improved to incorporate a better user interface.

CONCLUSION

In this paper we presented Bribecaster, a service that enables individuals in the developing world to safely and securely report and retrieve bribe-related transaction information. We presented new mechanisms that facilitate privacy control while simultaneously guarding against malicious reporting.

ACKNOWLEDGMENTS

We would like to thank Professor Björn Hartmann for continued support, discussion, advice and mentorship and Professor Eric Brewer for valuable suggestions. Wei Wu was instrumental in building the Android application. Steve Rubin played a key role in coding, user studies and documentation. Dinsha Mistree for valuable product suggestions. Professors Jennifer Bussell and Thad Dunning for ongoing collaboration in deploying Bribecaster in India, and studying the effects of such an intervention.

REFERENCES

[1] Bertrand, M., Djankov, S., Hanna, R. and Mullainathan, S. *Does corruption produce unsafe drivers?* , National Bureau of Economic Research, 2006.

[2] Treisman, D. What have we learned about the causes of corruption from ten years of cross-national empirical research? *Annu. Rev. Polit. Sci.*, 102007), 211-244.

[3] *Transparency International Annual Report 2010*. Transparency International, http://www.transparency.org/content/download/61964/992803, 2010.

[4] *IPaidABribe*. IPaidABribe.com.

[5] *Indians See Threat From Pakistan, Extremist Groups*. Pew Research Center, http://www.pewglobal.org/2010/10/20/indians-see-threat-from-pakistan-extremist-groups/, 2010.

[6] Basu, K. Why, for a Class of Bribes, the Act of Giving a Bribe should be Treated as Legal. *India Ministry of Finance Report* 2011.

[7] Abbink, K, Dasgupta, U., Gangadharan, L.and Jain, T, *Letting the Briber Go Free: An Experiment on Mitigating Harassment Bribes* .Indian School of Business WP ISB-WP/104/2012. (September 2013). Available at SSRN: http://ssrn.com/abstract=2166221 or http://dx.doi.org/10.2139/ssrn.2166221

[8] Mittal, M., Wu, W., Rubin, S., Madden, S., & Hartmann, B. (2012, February). Bribecaster: documenting bribes through community

participation. In *Proceedings of the ACM 2012 conference on Computer Supported Cooperative Work Companion* (pp. 171-174). ACM.

[9] *Bribespot*. bribespot.com.

[10] Jindal, N., & Liu, B. (2008, February). Opinion spam and analysis. In *Proceedings of the 2008 International Conference on Web Search and Data Mining* (pp. 219-230). ACM.

[11] Sassone, V., Hamadou, S. and Yang, M. *Trust in anonymity networks*. Springer, 2011.

[12] *Yelp's Review Filter Explained*. Yelp.com, http://officialblog.yelp.com/2010/03/yelp-review-filter-explained.html, 2010.

[13] *Yelp*. Yelp.com

[14] Monrose, F., & Rubin, A. D. (2000). Keystroke dynamics as a biometric for authentication. *Future Generation computer systems*, *16*(4), 351-359.

[15] Bleha, S., Slivinsky, C., & Hussien, B. (1990). Computer-access security systems using keystroke dynamics. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, *12*(12), 1217-1222.

[16] *Google Place API.* https://developers.google.com/places/documentation/

[17] *PyGeoIP.* https://pypi.python.org/pypi/pygeoip

[18] Bostock, M., Ogievetsky, V., & Heer, J. (2011). D³ data-driven documents. *Visualization and Computer Graphics, IEEE Transactions on*, *17*(12), 2301-2309.

[19] Amazon Mechanical Turk, https://www.mturk.com/mturk/welcome

[20] Kittur, A., Chi, E. H., & Suh, B. (2008, April). Crowdsourcing user studies with Mechanical Turk. In *Proceedings of the SIGCHI conference on human factors in computing systems* (pp. 453-456). ACM.

[21] Reicheld, F. F. The one number you need to grow. *Harvard Business Review*, 81, 12 2003), 46-55.

[22] Kohavi, R., Henne, R. M., & Sommerfield, D. (2007, August). Practical guide to controlled experiments on the web: listen to your customers not to the hippo. In *Proceedings of the 13th ACM SIGKDD international conference on Knowledge discovery and data mining* (pp. 959-967). ACM.

[23] Bussell, J., Dunning, T., & Mittal, M. (2014, March). *Reducing Corruption Through Crowdsourcing.* DIL Innovate Spring 2014 Proposal. Unpublished proposal, under review.

Appendix 1: Formative Survey

Corruption In India

This study is conducted by the University of California. We are exploring the use of technology to understand how it may be best used to combat corruption in India. Please answer the following questions to the best of your knowledge. © Manas Mittal, UC Berkeley, Computer Science.
manas@berkeley.edu

ALL YOUR RESPONSES WILL REMAIN ANONYMOUS.
TOTAL ESTIMATED TIME IS BETWEEN 12 - 15 MINUTES.

PAGE 1 of 3

* Required

Do you have or use: *

Please choose all that apply

- [ ] Mobile/Cell Phone
- [ ] Data Plan on Cell Phone
- [ ] SMS Plan on Cell Phone (Plans like send upto 50 messages for Rs. 10 a month)
- [ ] Smart Phone (Something that lets you access the internet, install apps, etc.)
- [ ] Facebook Account
- [ ] Computer at Home
- [ ] Internet at Home
- [ ] Computer at Work
- [ ] Internet at Work
- [ ] Internet at a Cyber Cafe
- [ ] Internet on your Cell/Mobile Phones
- [ ] None of the Above

If you have a Cell/Mobile Phone, Do you:

Skip this question if you don't have a cell phone. Please choose all that apply

- [ ] Send SMS'es to friends/relatives/people you know
- [ ] Receive SMS'es from friends/relatives/ people you know

Appendix 1: Formative Survey

- [ ] Send SMS'es to contests (such as TV contests, to vote for polls on News Channels etc.)
- [ ] Receive SMS'es about offers etc.
- [ ] If you receive SMS'es about offers etc., you find them useful.
- [ ] If you receive SMS'es about offers etc., you don't find them useful.
- [ ] Make & Receive phone calls

If you have a smartphone, Do you:
Skip this question if you don't have a smartphone, otherwise, please choose all that apply

- [ ] Download Apps
- [ ] Read Email on the Phone
- [ ] Send Email on the Phone
- [ ] Use the phone for "Google Maps" like application to look up where you are, or how to get to some place
- [ ] Use the smartphone to buy something online
- [ ] Access Facebook from the smartphone
- [ ] Read classified advertisements, etc.

If you have a smartphone, and if you download apps, can you tell us the names of 2 apps that use most often?

With reference to the 2 most commonly used apps, How did you find out about these?
Please choose all that apply

- [ ] From Friends
- [ ] From Family
- [ ] From TV Ad
- [ ] From Radio Ad
- [ ] From Newpaper / Print ad
- [ ] Read about it in a magazine
- [ ] Read about it in a Blog
- [ ] Found out on internet through other means (Like forums, etc)
- [ ] Other:

If you have a smartphone, What kind it is?

Appendix 1: Formative Survey

- ○ Android Phone
- ○ iPhone
- ○ Nokia Smartphone
- ○ Blackberry
- ○ Other: [ ]

If you don't have a smartphone, are you considering buying a smartphone? If so, What Type?

- ○ Android Phone
- ○ iPhone
- ○ Nokia Smartphone
- ○ Blackberry
- ○ Other: [ ]

Have you ever:
Please choose all that apply

- ☐ Read an online review of a product (like Washing Machine, or a book, or a movie), before buying it
- ☐ Read the newspaper online
- ☐ Written an online review
- ☐ Written a complaint online
- ☐ Purchased something online

How old are you? *

- ◉ < 18 years
- ○ 18 - 24 years
- ○ 24 - 36 years
- ○ 36 - 48 years
- ○ 48 - 60 years
- ○ 60+ years

Continue »

Appendix 1: Formative Survey

Corruption In India

Questions about Corruption in India (Page 2 of 3)

This study is conducted by the University of California, Berkeley. ALL YOUR RESPONSES WILL REMAIN ANONYMOUS. We are trying to understand if we can use technology to somehow expose every day corruption that happens everywhere in India. Please answer the following questions to the best of your knowledge.

Have you ever had to (or somebody on your behalf, like friends/relatives, had to):
Bribe is giving money or a expensive gifts in exchange of getting some work done. All answers are anonymous.

- ☐ Pay bribe to a Policeman.
- ☐ Pay bribe to Traffic Policeman
- ☐ Pay bribe to a Govt. Official.
- ☐ Pay bribe for getting a drivers license.
- ☐ Pay bribe for getting/repairing gas connection / water connection / telephone connection / getting Ration Cards
- ☐ Pay bribe for bending the rules
- ☐ Pay bribe for getting a job
- ☐ Pay bribe to a tax official
- ☐ Pay bribe for getting a Govt Contract?
- ☐ Pay bribe to get a Birth/Death cerficate
- ☐ Pay bribe to get a passport/Police Verification
- ☐ Pay bribe in other circumstances
- ☐ Pay bribe because Its Standard to pay bribes to get something done
- ☐ Other: _____

Have you ever had to (Or somebody on your behalf, like friends/relatives, had to):
Bribe is giving money or a expensive gifts in exchange of getting some work done. All answers are anonymous.

- ☐ Take bribe for personal gain
- ☐ Take bribe to buy gifts for my family
- ☐ Take bribe because its part of "the system"
- ☐ Take bribe because you are expected to pass a part of the bribe to other people.
- ☐ Other: _____

If you had to pay a bribe, how did you find the right amount to pay

Appendix 1: Formative Survey

- [ ] Agent or middleman told me
- [ ] The person who asked for the bribe told me how much to pay
- [ ] My friends/relatives told me
- [ ] They asked me to pay as much money I had (For example, if the police catches you).
- [ ] There is well known, practiced, standard amount (Like 5% of all inspection contracts, etc).
- [ ] Other:

Once you paid a bribe, how did you feel?

- [ ] Relived that the job will be done
- [ ] Frustrated or angry that you had to pay this bribe
- [ ] It is just part of the process, its standard, "I have accepted that I have to pay bribes".
- [ ] I felt cheated that I had to pay so much
- [ ] I felt relieved that I didn't have to pay so much.
- [ ] Other:

If you paid a bribe, did you feel that you had paid a 'Fair' price? Why or Why not?

Do you feel it is important to clean low-level corruption (like policeman, etc) before trying to deal with politicians at higher levels?

« Back Continue »

Appendix 1: Formative Survey

Corruption In India

* Required

Do you Complain? (Page 3 of 3)

Once you paid a bribe, did you tell your friends/relatives about it?

- [ ] No, because it is embarrassing that I had to pay money
- [ ] No, because I got such a good deal
- [ ] No, because its just part of the system
- [ ] No, because there is no reason to tell
- [ ] No, because its standard
- [ ] No, for some other reason
- [ ] Yes, because I felt bad paying for the bribe
- [ ] Yes, because I felt cheated
- [ ] Yes, so that they are informed
- [ ] Yes, this is standard business practice, and establishes the norm
- [ ] Yes, because thats standard-
- [ ] Other:

Have you ever complained about a bribe?

- [ ] Yes, to a more senior person
- [ ] Yes, to a Lokayukta
- [ ] Yes, to Media (Newspapers, TV, etc)
- [ ] Yes, to Vigilance Department
- [ ] Yes, to the Police
- [ ] No, I have accepted it as a part of the system.
- [ ] No, If I complain, the work will not get done
- [ ] No, If I complain, the person I have bribed will get to know about it, and come after me
- [ ] No, some other reason
- [ ] Other:

Have you ever complained about

- [ ] Problem with the Telephone Connection (To Senior Telephone Company Officials)
- [ ] Problem with the Water Connection (To Senior Water Supply Company)
- [ ] Problems Electricity Connection (To Electricity Company People)

Appendix 1: Formative Survey

- [ ] Problems with Roads
- [ ] Problems with a Consumer Product you purchased (like TV, Washing Machine, etc) to Shop keeper or Company whose product it was
- [ ] Problems with a Consumer Product you purchased (like TV, Washing Machine, etc) to Consumer Forum / Customer Court
- [ ] Informed your friends and relatives to never buy a product of a specific company (Like, Godrej, etc) based on Poor Service
- [ ] Other:

If it would help you and other people, and it was easy to do, would you anonymously report bribes you paid to get something done? Please write any thoughts you might have about this matter. *

If information about how much Bribe to pay, and to whom, to get some work done was available online (or on your phone), would you trust and use this information. Please explain any concerns you might have. *

If you could anonymously report bribes through a online web-site or a SmartPhone App, Would you be willing to do so? *

Have you ever heard about ipaidabribe.com, if so, have you used it. Did you like or dislike something about it?

Appendix 1: Formative Survey

Please enter the current (local) time. Also enter the same time in the mechanical turk form. We will use this time so that we can link responses between here and Mechanical Turk and pay. *

For example, enter "12:24" pm here and enter the same on the mechanical turk

PLEASE CLICK SUBMIT. REMEMBER TO ENTER THE TIME (AS FILLED IN THE LAST QUESTION) IN MECHANICAL TURK.

« Back Submit

Never submit passwords through Google Forms.

Powered by Google Docs

Report Abuse - Terms of Service - Additional Terms

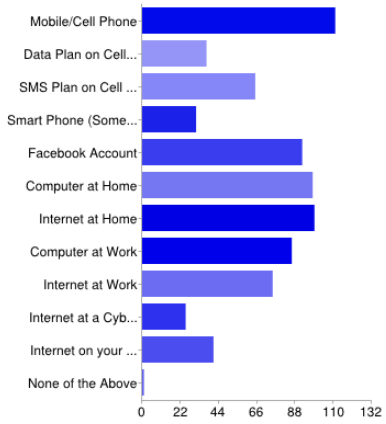
Appendix 2: Results of Formative Survey

102 Respondents completed all three pages of the survey. 116 respondents completed page 1.

Summary

See complete responses

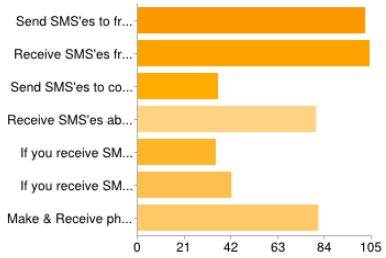
Do you have or use:



Mobile/Cell Phone	**111**	96%
Data Plan on Cell Phone	**37**	32%
SMS Plan on Cell Phone (Plans like send upto 50 messages for Rs. 10 a month)	**65**	56%
Smart Phone (Something that lets you access the internet, install apps, etc.)	**31**	27%
Facebook Account	**92**	79%
Computer at Home	**98**	84%
Internet at Home	**99**	85%
Computer at Work	**86**	74%
Internet at Work	**75**	65%
Internet at a Cyber Cafe	**25**	22%
Internet on your Cell/Mobile Phones	**41**	35%
None of the Above	**1**	1%

People may select more than one checkbox, so percentages may add up to more than 100%.

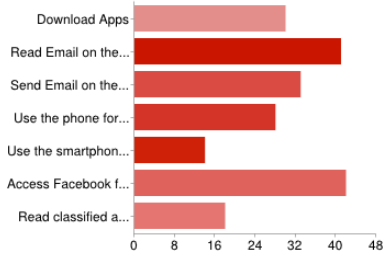
If you have a Cell/Mobile Phone, Do you:



Send SMS'es to friends/relatives/people you know	**102**	90%
Receive SMS'es from friends/relatives/ people you know	**104**	92%
Send SMS'es to contests (such as TV contests, to vote for polls on News Channels etc.)	**36**	32%
Receive SMS'es about offers etc.	**80**	71%
If you receive SMS'es about offers etc., you find them useful.	**35**	31%
If you receive SMS'es about offers etc., you don't find them useful.	**42**	37%
Make & Receive phone calls	**81**	72%

People may select more than one checkbox, so percentages may add up to more than 100%.

If you have a smartphone, Do you:

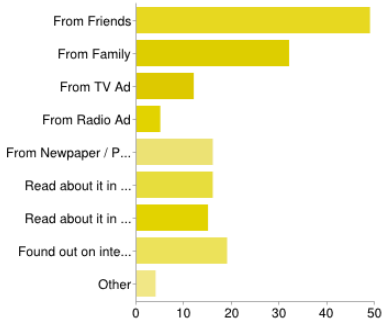


Download Apps	**30**	52%
Read Email on the Phone	**41**	71%
Send Email on the Phone	**33**	57%
Use the phone for "Google Maps" like application to look up where you are, or how to get to some place	**28**	48%
Use the smartphone to buy something online	**14**	24%
Access Facebook from the smartphone	**42**	72%
Read classified advertisements, etc.	**18**	31%

People may select more than one checkbox, so percentages may add up to more than 100%.

Appendix 2: Results of Formative Survey

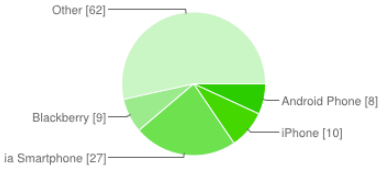
With reference to the 2 most commonly used apps, How did you find out about these?



From Friends	**49**	68%
From Family	**32**	44%
From TV Ad	**12**	17%
From Radio Ad	**5**	7%
From Newpaper / Print ad	**16**	22%
Read about it in a magazine	**16**	22%
Read about it in a Blog	**15**	21%
Found out on internet through other means (Like forums, etc)	**19**	26%
Other	**4**	6%

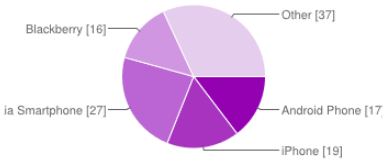
People may select more than one checkbox, so percentages may add up to more than 100%.

If you have a smartphone, What kind it is?



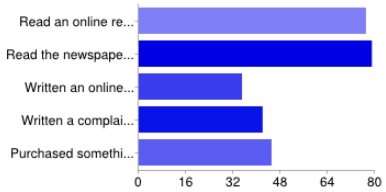
Android Phone	**8**	7%
iPhone	**10**	9%
Nokia Smartphone	**27**	23%
Blackberry	**9**	8%
Other	**62**	53%

If you don't have a smartphone, are you considering buying a smartphone? If so, What Type?



Android Phone	**17**	15%
iPhone	**19**	16%
Nokia Smartphone	**27**	23%
Blackberry	**16**	14%
Other	**37**	32%

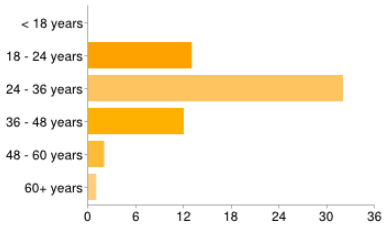
Have you ever:



Read an online review of a product (like Washing Machine, or a book, or a movie), before buying it	**77**	76%
Read the newspaper online	**79**	78%
Written an online review	**35**	35%
Written a complaint online	**42**	42%
Purchased something online	**45**	45%

People may select more than one checkbox, so percentages may add up to more than 100%.

How old are you?



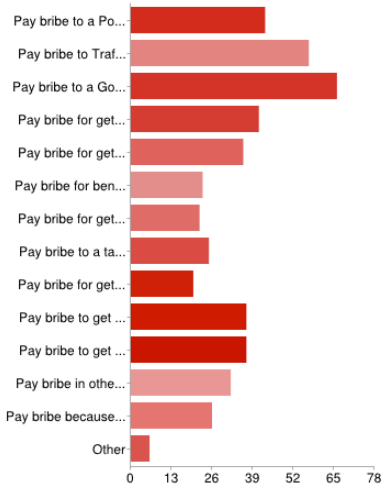
< 18 years	**0**	0%
18 - 24 years	**13**	11%
24 - 36 years	**32**	28%
36 - 48 years	**12**	10%
48 - 60 years	**2**	2%
60+ years	**1**	1%

Appendix 2: Results of Formative Survey

Questions about Corruption in India (Page 2 of 3)

This study is conducted by the University of California, Berkeley. ALL YOUR RESPONSES WILL REMAIN ANONYMOUS. We are trying to understand if we can use technology to somehow expose every day corruption that happens everywhere in India. Please answer the following questions to the best of your knowledge.

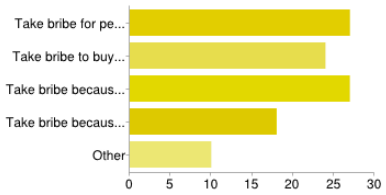
Have you ever had to (or somebody on your behalf, like friends/relatives, had to):



Pay bribe to a Policeman.	43
Pay bribe to Traffic Policeman	57
Pay bribe to a Govt. Official.	66
Pay bribe for getting a drivers license.	41
Pay bribe for getting/repairing gas connection / water connection / telephone connection / getting Ration Cards	36
Pay bribe for bending the rules	23
Pay bribe for getting a job	22
Pay bribe to a tax official	25
Pay bribe for getting a Govt Contract?	20
Pay bribe to get a Birth/Death cerficate	37
Pay bribe to get a passport/Police Verification	37
Pay bribe in other circumstances	32
Pay bribe because Its Standard to pay bribes to get something done	26
Other	6

People may select more than one checkbox, so percentages may add up to more than 100%.

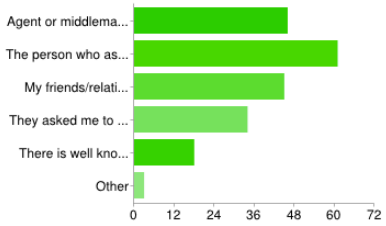
Have you ever had to (Or somebody on your behalf, like friends/relatives, had to):



Take bribe for personal gain	27	39%
Take bribe to buy gifts for my family	24	34%
Take bribe because its part of "the system"	27	39%
Take bribe because you are expected to pass a part of the bribe to other people.	18	26%
Other	10	14%

People may select more than one checkbox, so percentages may add up to more than 100%.

If you had to pay a bribe, how did you find the right amount to pay



Agent or middleman told me	46	43%
The person who asked for the bribe told me how much to pay	61	58%
My friends/relatives told me	45	42%
They asked me to pay as much money I had (For example, if the police catches you).	34	32%
There is well known, practiced, standard amount (Like 5% of all inspection contracts, etc).	18	17%
Other	3	3%

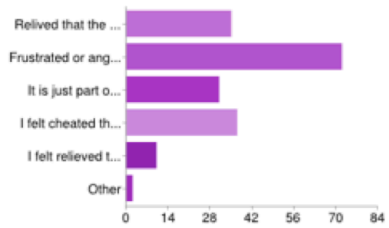
People may select more than one checkbox, so percentages may add up to more than 100%.

Once you paid a bribe, how did you feel?

Relived that the job will be done	35	33%
Frustrated or angry that you had to pay this bribe	72	68%
It is just part of the process, its standard, "I have accepted that I have to pay bribes".	31	29%
I felt cheated that I had to pay so much	37	35%
I felt relieved that I didn't have to pay so much.	10	9%
Other	2	2%

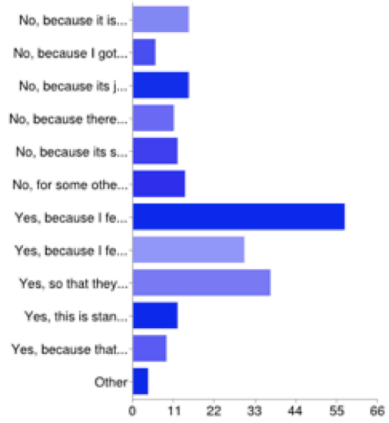
People may select more than one checkbox, so percentages may add up to more than 100%.

Appendix 2: Results of Formative Survey



Do you Complain? (Page 3 of 3)

Once you paid a bribe, did you tell your friends/relatives about it?



No, because it is embarrassing that I had to pay money	**15**	14%
No, because I got such a good deal	**6**	6%
No, because its just part of the system	**15**	14%
No, because there is no reason to tell	**11**	10%
No, because its standard	**12**	11%
No, for some other reason	**14**	13%
Yes, because I felt bad paying for the bribe	**57**	52%
Yes, because I felt cheated	**30**	28%
Yes, so that they are informed	**37**	34%
Yes, this is standard business practice, and establishes the norm	**12**	11%
Yes, because thats standard-	**9**	8%
Other	**4**	4%

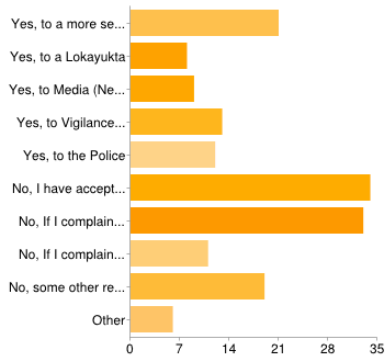
People may select more than one checkbox, so percentages may add up to more than 100%.

Have you ever complained about a bribe?

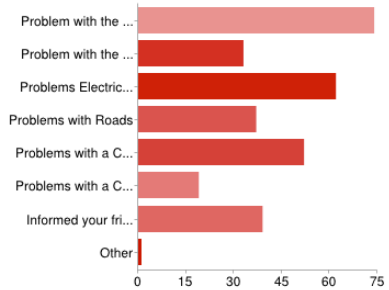
Yes, to a more senior person	**21**	19%
Yes, to a Lokayukta	**8**	7%
Yes, to Media (Newspapers, TV, etc)	**9**	8%
Yes, to Vigilance Department	**13**	12%
Yes, to the Police	**12**	11%
No, I have accepted it as a part of the system.	**34**	31%
No, If I complain, the work will not get done	**33**	30%
No, If I complain, the person I have bribed will get to know about it, and come after me	**11**	10%
No, some other reason	**19**	17%
Other	**6**	6%

People may select more than one checkbox, so percentages may add up to more than 100%.

Appendix 2: Results of Formative Survey



Have you ever complained about



Problem with the Telephone Connection (To Senior Telephone Company Officials)
Problem with the Water Connection (To Senior Water Supply Company)
Problems Electricity Connection (To Electricity Company People)
Problems with Roads
Problems with a Consumer Product you purchased (like TV, Washing Machine, etc) to Shop keeper or Company whos
Problems with a Consumer Product you purchased (like TV, Washing Machine, etc) to Consumer Forum / Customer Cc
Informed your friends and relatives to never buy a product of a specific company (Like, Godrej, etc) based on Poor Serv
Other

People may select more than one checkbox, so percentages may add up to more than 100%.

Appendix 3: Usefulness, Usability & NPS Survey (Post - Task)

Short Bribecaster Survey (V0.2)

Please answer the following questions. At the end of the page, you will see a code that you need to enter into Amazon Mechanical Turk.
* Required

Please indicate your opinions on the following statements *

	1 - Strongly Disagree (Strong NO)	2 - Disagree	3 - Neutral	4 - Agree	5 - Strongly Agree (Strong YES)
Privacy is a big concern when reporting corruption or/and bribe related information	○	○	○	○	○
I feel safe and anonymous when reporting bribe transactions on the Bribecaster system	○	○	○	○	○
I would feel safe writing the names of officials on Bribecaster	○	○	○	○	○
I would be comfortable relying on information that other people have submitted	○	○	○	○	○

Did you feel safe and anonymous when reporting bribe transactions on Bribecaster -- why or why not? *
Please explain

How likely are you to recommend Bribecaster to a friend, colleague, or relative? *

	0	1	2	3	4	5	6	7	8	9	10	
Not at all likely	○	○	○	○	○	○	○	○	○	○	○	Very likely

Please enter the following code in Amazon Mechanical Turk *
This will help us identify that it's you, and pay you appropriately

Appendix 4: Results of Usefulness, Usability & NPS Survey (Post - Task)

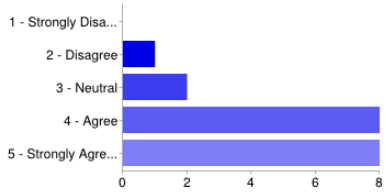
This form will soon be upgraded to the new version of Google Forms. Learn more.

19 responses

Summary

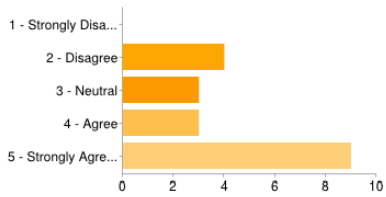
See complete responses

Please indicate your opinions on the following statements - Privacy is a big concern when reporting corruption or/and bribe related information



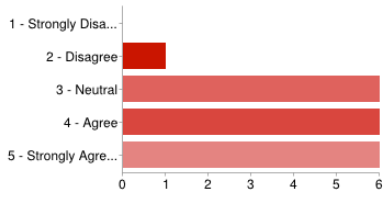
1 - Strongly Disagree (Strong NO)	0	0%
2 - Disagree	1	5%
3 - Neutral	2	11%
4 - Agree	8	42%
5 - Strongly Agree (Strong YES)	8	42%

Please indicate your opinions on the following statements - I feel safe and anonymous when reporting bribe transactions on the Bribecaster system



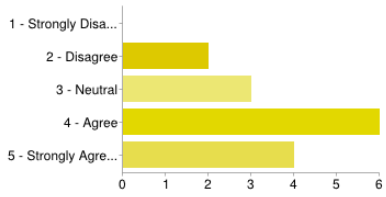
1 - Strongly Disagree (Strong NO)	0	0%
2 - Disagree	4	21%
3 - Neutral	3	16%
4 - Agree	3	16%
5 - Strongly Agree (Strong YES)	9	47%

Please indicate your opinions on the following statements - I would feel safe writing the names of officials on Bribecaster



1 - Strongly Disagree (Strong NO)	0	0%
2 - Disagree	1	5%
3 - Neutral	6	32%
4 - Agree	6	32%
5 - Strongly Agree (Strong YES)	6	32%

Please indicate your opinions on the following statements - I would be comfortable relying on information that other people have submitted



1 - Strongly Disagree (Strong NO)	0	0%
2 - Disagree	2	11%
3 - Neutral	3	16%
4 - Agree	6	32%
5 - Strongly Agree (Strong YES)	4	21%

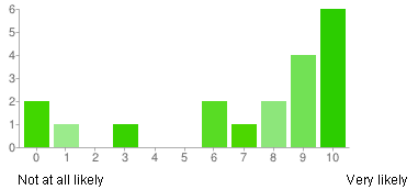
Did you feel safe and anonymous when reporting bribe transactions on Bribecaster -- why or why not?

I FEEL SAFE WHEN REPORTING BRIDE ,BECAUSE NOW A DAYS MEDIAS ARE VERY WEAR TO REPORT THE SAME ON TELECAST. I did n't give any personal information and also seeing this website i am very confident that it is very safe. Still now i didnt pay anny bribe to RTO. But they didnt issue Driving License in a particular time, because of bribe they extend and give on longer time. I feel this not safe, we must destroy the bribe and give heavy punishment, who involved in bribe. Not much because they asked for full name and location. Because the site seems to more trustworthy and reliable. Yes, I feel safe ...

How likely are you to recommend Bribecaster to a friend, colleague, or relative?

0 - Not at all likely	2	11%

Appendix 4: Results of Usefulness, Usability & NPS Survey (Post - Task)



1	**1**	5%
2	**0**	0%
3	**1**	5%
4	**0**	0%
5	**0**	0%
6	**2**	11%
7	**1**	5%
8	**2**	11%
9	**4**	21%
10 - Very likely	**6**	32%