Escaping from Government and Corporate Surveillance. Evidence from the MIT Digital Currency Experiment

Susan Athey, Christian Catalini, and Catherine Tucker*

October 3, 2016

Abstract

This paper uses data from the MIT digital currency experiment to shed light on consumer behavior regarding commercial and government surveillance. This allows us to explore the apparent contradiction that many cryptocurrencies offer people the chance to escape government surveillance, but do so by making transactions themselves public. We find three main things. First, the effect of small incentives (financial or otherwise) may explain the privacy paradox, where people say they care about privacy but are willing to relinquish private data to firms quite easily. Second, prompts about government surveillance can lead consumers to be be more protective about linking their personal identity to their digital wallets, but such privacy enhancing behavior is suppressed in the presence of irrelevant but reassuring information about privacy protection. Third, that we also see such irrelevant but reassuring information lead consumers to be less likely to take more general actions to escape surveillance at large.

*Susan Athey: Graduate School of Business, Stanford University, and NBER. Christian Catalini: MIT Sloan School of Management, MIT. Catherine Tucker: MIT Sloan School of Management, MIT and NBER. Corresponding author: catalini@mit.edu

1 Summary of Main Results

In the Fall of 2014, students at the Massachusetts Institute of Technology were preparing for one of the largest social science experiments the campus had seen (Catalini and Tucker, 2016): In the following weeks, every undergraduate student would be given $100 worth of Bitcoin, the first decentralized cryptocurrency to solve the double-spending problem that had plagued computer scientists' early attempts at creating digital cash (Nakamoto, 2008; Narayanan et al., 2016).

As part of the experiment students would have to select a digital wallet, create a Bitcoin address to receive the funds, and learn about encryption (PGP) to secure their incoming bitcoin. At multiple points in the process they not only faced trade-offs between privacy, security and convenience, but also had to make choices in terms of who could have access to their transactions data in the future.

We find three main things. First, the effect of small incentives (financial or otherwise) may explain the privacy paradox, where people say they care about privacy but are willing to relinquish private data to firms quite easily. Second, prompts about government surveillance can lead consumers to be be more protective about linking their personal identity to their digital wallets, but such privacy enhancing behavior is suppressed in the presence of irrelevant but reassuring information about privacy protection. Third, that we also see such irrelevant but reassuring information lead consumers to be less likely to take more general actions to escape surveillance at large. In the following sections, we briefly discuss each one of these findings in more detail.

1.1 Privacy Paradox

1.1.1 Small Frictions and Privacy Trade-Offs in Digital Wallets

During the sign-up process students had to learn about data security, and were offered the opportunity to encrypt and sign the Bitcoin address they intended to use for the distribution for additional security and privacy. Whereas the majority of participants (55%) tried this additional step, only 49% of those who tried succeeded, with the others falling back to the easier flow without encryption.

The wallet selections of participants are also informative about their privacy preferences. Whereas open-source Bitcoin wallets like Electrum offer a high degree of privacy from the government and do not require an intermediary to be used, they also record all transactions on the Bitcoin public ledger (i.e. the blockchain) under a pseudonym. While users can technically generate a new pseudonym (i.e. a new Bitcoin address) for each new transaction, over time patterns of transactions can be analyzed to de-anonymize users unless additional steps (e.g. mixing transactions with multiple users) are taken to make tracking more difficult. In a recent study of Bitcoin adoption and usage, Athey et al. (2016), after using different heuristics and public data sources to map pseudonyms to individual entities, are able to track analyze individual transaction patterns over time (e.g. trading, international money transfer, gambling etc.). Their results highlight how investing (store of value) is to date the predominant use of Bitcoin.

Open source wallets also tend to be less user friendly and convenient to use relative to more 'bank-like' digital wallets like Circle or Coinbase. Bank-like wallets connect to traditional bank accounts and credit cards, offer a mobile app, can easily convert Bitcoin to and from fiat-money, and may provide additional privacy to their users because of the way they generate new pseudonyms for each transaction, or pool transactions within their network without recording each one of them on the public Bitcoin ledger (off-chain transactions).

At the same time, with bank-like wallets users need to be comfortable sharing all their transaction data and identity information with a startup and possibly the government (since digital wallet intermediaries needs to comply with Anti-Money Laundering (AML) and Know Your Customer (KYC) regulations like any other financial institutions).

Similar to what we observe with encryption, convenience dominates wallet choices. The vast majority of participants (74%) selected a bank-like wallet over an open source alternative, i.e. they accepted potential corporate and government surveillance in exchange for ease of use. Their choice was also strongly affected by the random order of wallets they were exposed to during the sign-up process: when a bank-like wallet was listed first among the options, 78% of students selected it (as opposed to only 65% when it was listed 2nd or lower); when the Electrum wallet (fully open-source) was listed first, 12% of students chose it (compared to only 8% when it was not).

Therefore small additional frictions, such as those generated by a lower ranking in a list of only four wallets, generated large differences in terms of digital wallet privacy choices.

Furthermore, when we randomly highlighted the possibility of government surveillance on Bitcoin transactions, students increased their propensity to use a fully open-source wallet from 7.3% to 10.9% (p= 0.0005). Interestingly, under the same randomization, the share of students that selected a bank-like wallet with privacy-enhancing features also increased by 14% (from 64.2% to 78.3%, p= 0.0000). Overall, the government surveillance nudge had two effects on wallet choices: it shifted some participants towards wallets that cannot be easily tracked by the government, and pushed others towards bank-like products that offer increased protection from public tracking on the Bitcoin ledger (while at the same time revealing all transactions to an intermediary).

1.1.2 Privacy of Your Contacts and Incentives

When asked by the National Cyber Security Alliance (NCSA) in a survey[1], 60% consumers stated that they would never feel comfortable sharing their list of contacts when asked. Moreover, in the same survey information about one's contacts ranked as the second most private piece of information for consumers, right after social security numbers (68% would never share them when asked).

Results from the MIT digital currency study allow us to compare these stated preferences to revealed preferences (at least for our study sample). In particular, we can verify if participants gave us fake emails during sign-up when we asked them about their friends versus not, and how one of our randomizations - an incentive in exchange for your friends' emails - affected their propensity to ultimately protect the privacy of their friends.

In Figure 1 the dependent variable is equal to one if all the emails provided by a student are invalid, and zero otherwise. 'Ask' refers to the condition where we simply asked for the friends' emails as part of one of the steps of the sign-up process. Under the 'Ask' condition, no incentive was provided to fill the email addresses. 'Ask + Incentive' refers to the condition where we asked the students for their friends' emails in combination with the possibility of receiving a pizza to share with them. This incentivized condition was offered to 50% of our sample.

Within the sample exposed to the incentive, 5% of students gave all invalid emails under 'Ask', and 2.4% under 'Ask + Incentive'. Within the full sample, 6% of students gave all invalid emails under the 'Ask' condition. In Figure 2, heterogeneous effects by gender, cohort of study, digital wallet selected, expectations about bitcoin, coding skills and operating system show an extremely consistent response to the incentive across groups.

Under the 'Ask + Incentive' treatment, students are substantially more likely to reveal

[1]https://staysafeonline.org/about-us/news/results-of-consumer-data-privacy-survey-reveal-critical-need-for-all-digital-citizens-to-participate-in-data-privacy-day

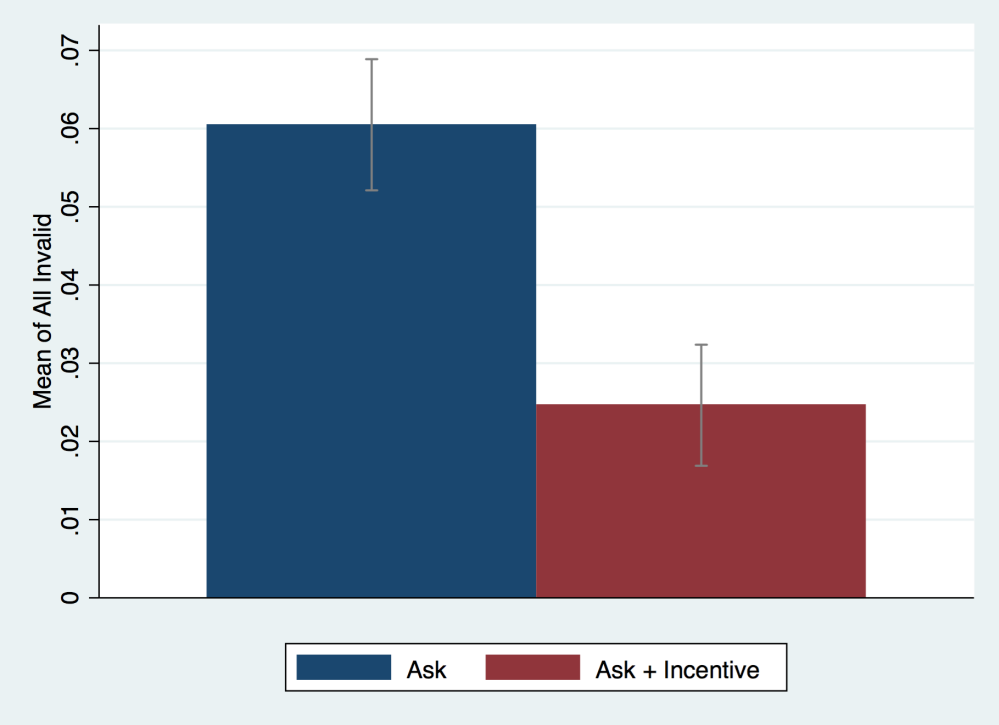


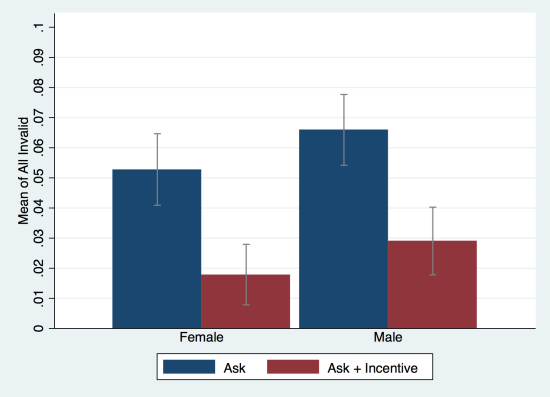
Figure 1: Effect of Incentives on Invalid Emails

the emails of their friends. I.e. while people say they care about privacy, they are also willing to relinquish private data quite easily when incentivized to do so.

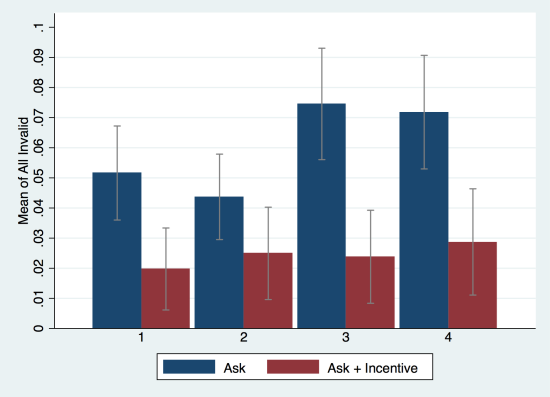
1.2 Government and Corporate Surveillance

For bank-like digital wallets, we are able to verify if participants decide to link their Bitcoin wallet to a traditional bank account, possibly making it easier for the government to track their transactions in the digital currency.

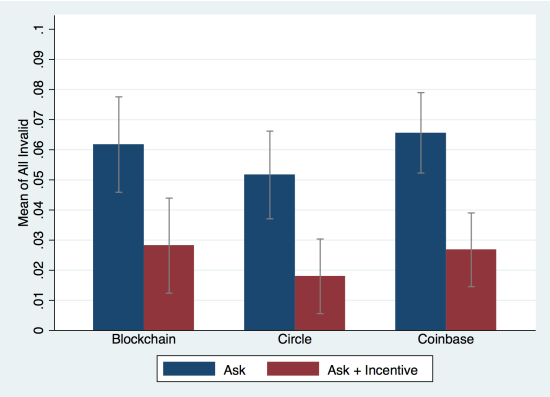
The dependent variable in Figure 3 is equal to one if students linked their digital wallet to a traditional bank account and zero otherwise. The sample excludes students who converted all their Bitcoin to US dollars (since linking to a bank account could be a necessary step towards cashing out). Under the 'Wallets' condition (50% of sample) students were only shown the list of wallets. Under the 'Wallets + Surveillance Nudge Randomization' (50% of



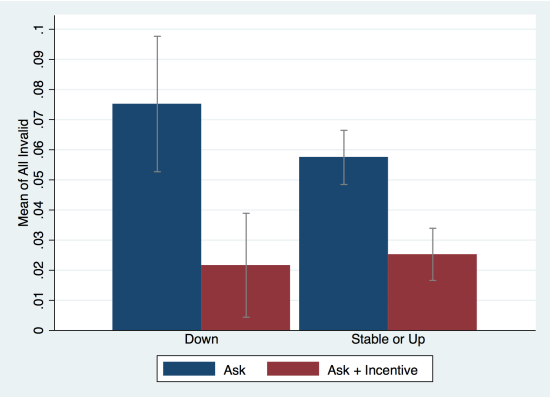
(a) Gender



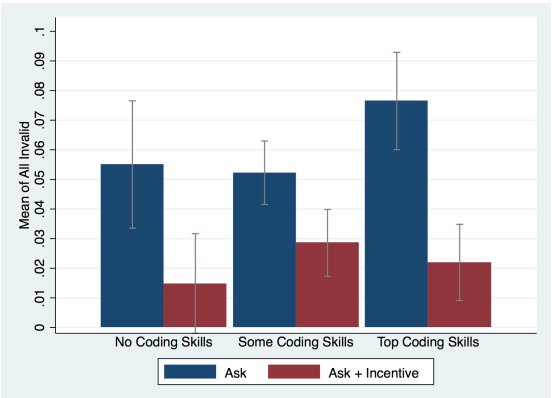
(b) Year of Study



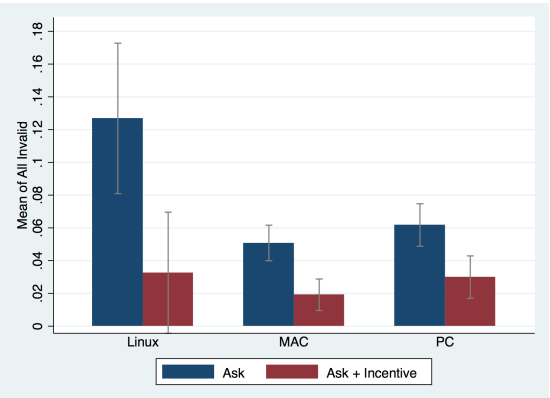
(c) Digital Wallet Preferences



(d) Expectations About Bitcoin Price



(e) Coding Ability



(f) Operating System

Figure 2: Effect of Incentives on Invalid Emails - Absence of Heterogeneous Effects

sample) students were also shown additional information about the ability of the government to track transactions made using the different wallets.

Under the 'Encryption Randomization' (50% of sample), students were exposed to a longer text describing PGP, and how the technology can be used to avoid eavesdropping and secure communications. While PGP technology is a useful privacy-enhancing tool, in our context it did not have a direct effect on the privacy of the participants' transactions, i.e. it constituted irrelevant, but possibly reassuring information about privacy protection.

As can be seen in Figure 3, when reminded about government surveillance, students are less likely to link their digital wallet to a traditional bank account, i.e. they are more proactive in protecting their privacy from the government (compare bars 1 and 3 in the graph) . At the same time, such privacy protective behavior disappears under the 'Encryption Randomization' (the last bar in Figure 3) , i.e. when the students were shown irrelevant, but reassuring information about privacy protection. The illusion of protection arising from the 'Encryption Randomization' reverts the participants' behavior to the baseline outcome we observe in the absence of the government surveillance randomization.

The 'Encryption Randomization' has a similar effect on general actions participants engage in to escape surveillance at large (i.e. above and beyond the action of linking the digital wallet to a traditional bank account).

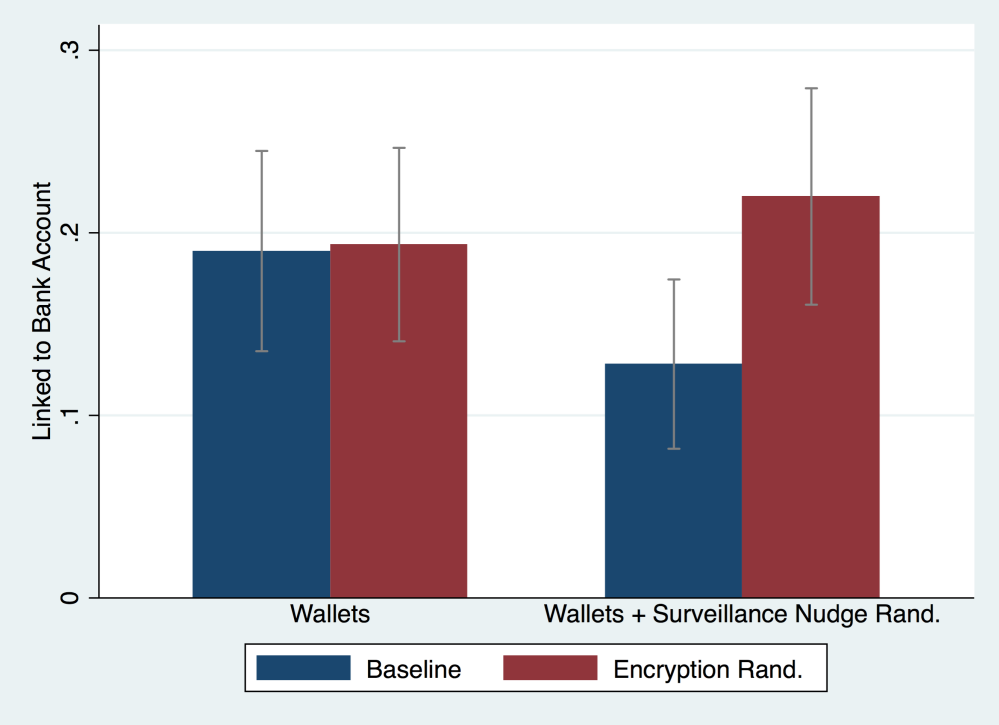


Figure 3: Effect of Government Surveillance Nudge Randomization and Encryption Randomization on Disclosure to the Government

References

Athey, S., I. Parashkevov, S. Sarukkai, and J. Xia (2016). Bitcoin pricing, adoption, and usage: Theory and evidence. *SSRN Working Paper No. 2822729, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2822729*.

Catalini, C. and C. Tucker (2016). Seeding the s-curve? the role of early adopters in diffusion. *SSRN Working Paper No. 28266749, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=28266749*.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *https://bitcoin.org/bitcoin.pdf*.

Narayanan, A., J. Bonneau, E. Felten, A. Miller, and S. Goldfeder (2016). *Bitcoin and Cryptocurrency Technologies*. Princeton University Press: Princeton NJ.