The Digital Privacy Paradox:
Small Money, Small Costs, Small Talk

Susan Athey
Stanford

Christian Catalini
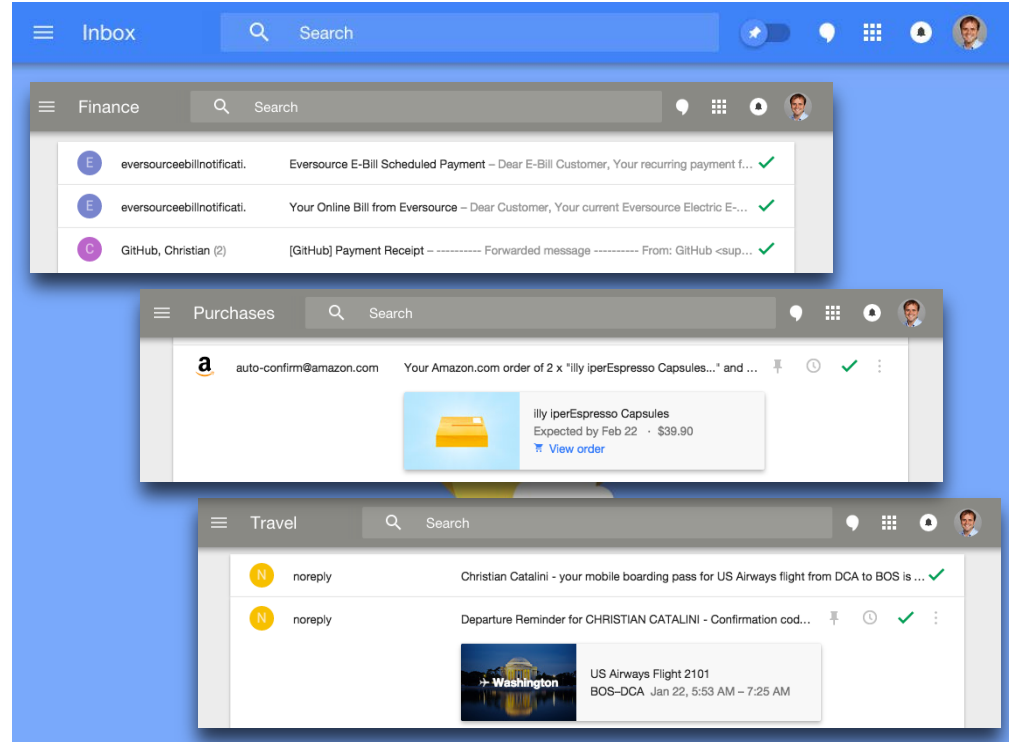MIT

Catherine Tucker
MIT

PrivacyCon
February 28th, 2018

PRIVACYCON

Why Do People Say They Care About Privacy and Government Surveillance…

But Then Share Personal Data with Firms…

…and Knowingly Use Technologies That Do Not Safeguard their Privacy

Unpacking The Privacy Paradox

- What can we learn from the MIT Digital Currency Experiment about these apparent privacy paradoxes?

- This is not a paper about digital currency per se… although a key promise of blockchain and cryptocurrencies is improved digital privacy!

- Surprisingly little economics work on the malleability of privacy preferences (Acquisti is the exception)

- Background policy question:
  - What are we trying to regulate?
  - What are we trying to protect consumers from?

The MIT Digital Currency Experiment
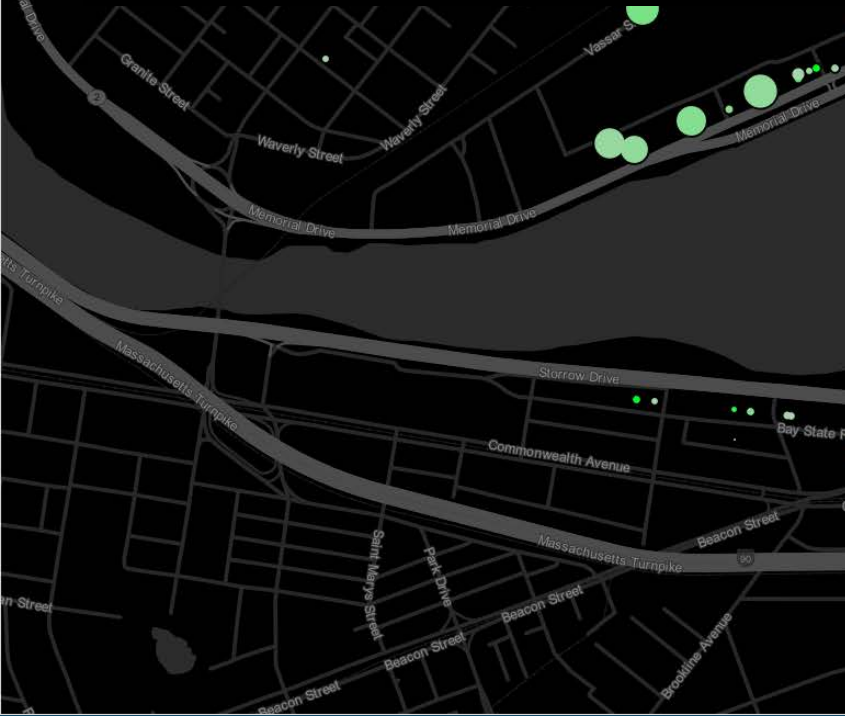
- ~5,000 students eligible. Survey on privacy preferences, digital payments etc

- 3 randomizations and related privacy choices and outcomes. Students had to select/generate a digital wallet, learn about encryption

- Key Findings: small incentives, small costs and small talk lead participants to ignore their privacy preferences (both stated, and past revealed)
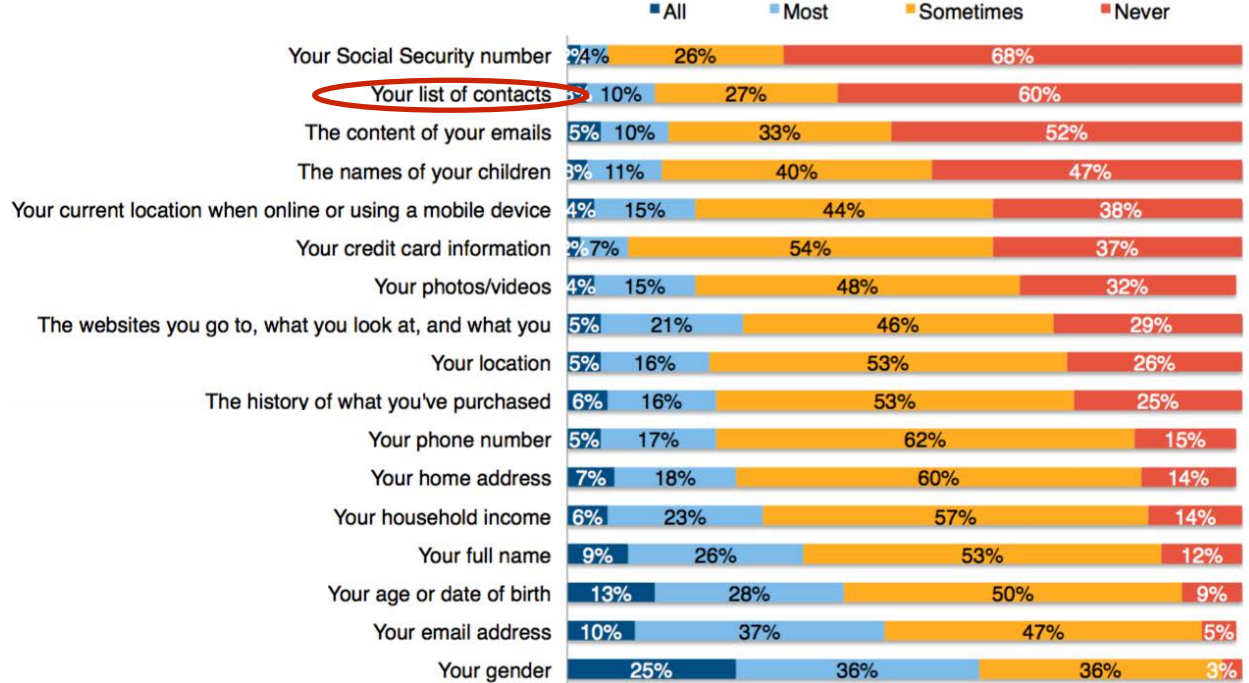
1. Small Money

Whereas people say they care about privacy, they are willing to relinquish private data quite easily…

We asked for the emails of the students' closest friends. However, it turns out that this is some of the personal data that is considered most private…

At Least in Surveys…

Source: National Cyber Security Alliance (2014), N=493

PRIVACYCON

… in Print and Lawsuits

News Video Events CrunchBase

DISRUPT LONDON BlaBlaCar Co-Founder And COO, Nicolas Brusson, To Speak At Disrupt London
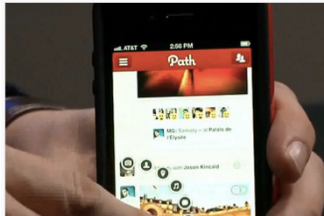Save £400 On Tickets Now ▶

Apps path

The Wrong Way: Path Uploads iOS Users' Address Books Without Permission

Posted Feb 7, 2012 by Chris Velazco (@chrisvelazco)

1,288 SHARES

What started as a bit of aimless tinkering for developer Arun Thampi ultimately unearthed something very surprising about personal life-sharing service Path. As a fan of the app, Thampi took it upon himself to look at the API calls that the app made to Path's service and found that his "entire address book (including full names, emails and phone numbers) was being sent as a plist to Path."
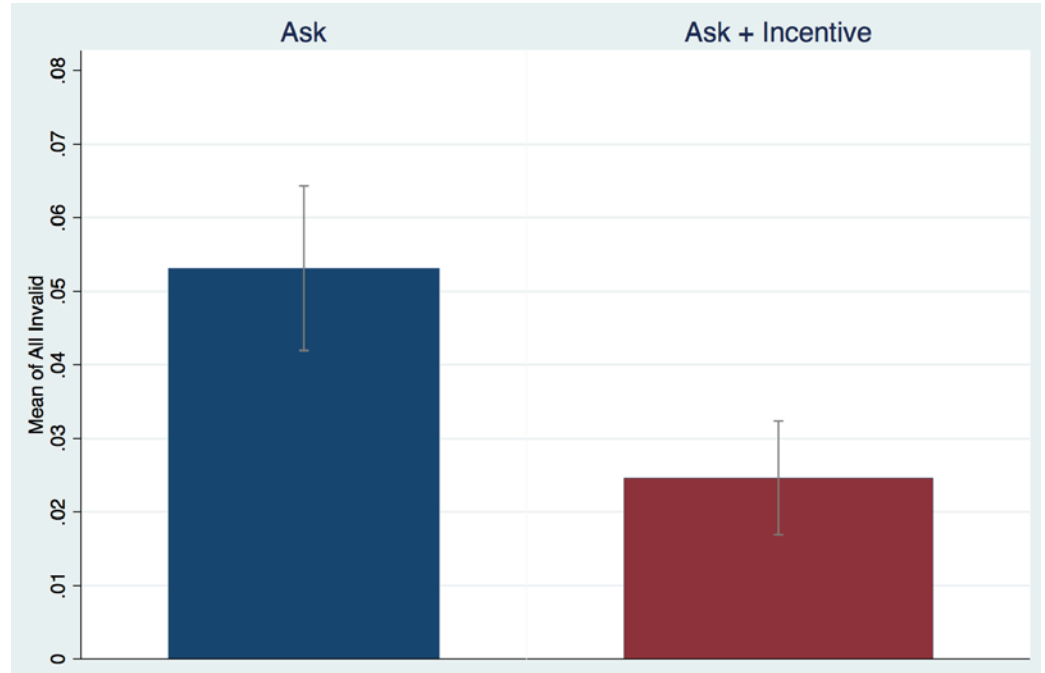

LinkedIn will pay $13M for sending those awful emails

by Jeff John Roberts   @jeffjohnroberts   OCTOBER 5, 2015, 8:23 AM EDT

Random 50% of the Sample: Pizza
In Exchange For Their Closest Friends' Emails

Do You Protect the Privacy of Your Friends?

54% decrease

VARIABLES	(1) All Invalid	(2) All Invalid	(3) All Invalid	(4) All Invalid	(5) All Invalid	(6) All Invalid	(7) All Invalid
Ask + Incentive (AI)	-0.0285*** (0.0059)	-0.0268*** (0.0066)	-0.0224*** (0.0076)	-0.0249*** (0.0068)	-0.0245*** (0.0074)	-0.0327*** (0.0060)	-0.0332*** (0.0066)
AI × Above Median Privacy Public		-0.0045 (0.0079)					
AI × Above Median Privacy Intermediary			-0.0110 (0.0081)				
AI × Above Median Privacy Government				-0.0085 (0.0078)			
AI × Above Median Trust Government					-0.0080 (0.0079)		
AI × Above Median Trust Startup						0.0153 (0.0100)	
AI × Above Median Trust Retailer							0.0105 (0.0081)
Constant	0.0531*** (0.0057)	0.0531*** (0.0057)	0.0531*** (0.0057)	0.0531*** (0.0057)	0.0531*** (0.0057)	0.0531*** (0.0057)	0.0531*** (0.0057)
Observations	3,086	3,086	3,086	3,086	3,086	3,086	3,086
R-squared	0.005	0.006	0.006	0.006	0.006	0.006	0.006

Heterogeneous Effects? None!

- Gender
- Race
- Citizenship Status
- Year of Study
- Coding Ability
- Digital Wallet Preference
- Will the Bitcoin price go down?
- Are you a Mac or a PC?
- Privacy Sensitive
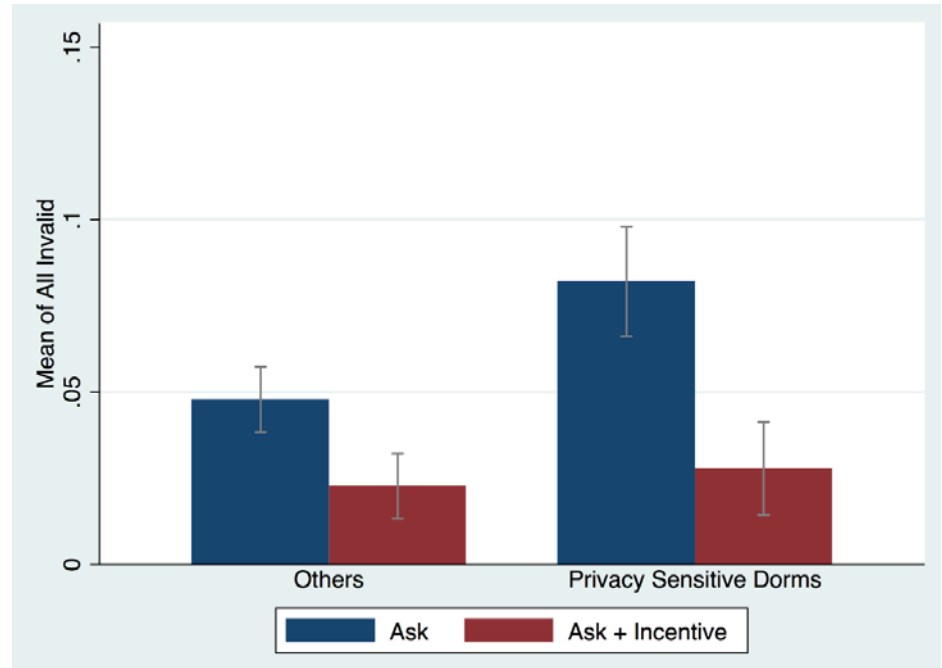
PRIVACYCON

2. Small Costs

Small frictions in the process of selecting a new technology, have large effects on privacy choices.

Inspired by the Microsoft Windows "Browser Ballot" Screen

- Wallets differ in terms of how much they expose a user's transactions to an intermediary, the government and the public

- Random Order

- Increased Transparency: 50% randomly exposed to additional information on key trade-offs

VARIABLES	(1) Maximized Privacy from the Public	(2) Maximized Privacy from the Public	(3) Maximized Privacy from the Intermediary	(4) Maximized Privacy from the Intermediary	(5) Maximized Privacy from the Government	(6) Maximized Privacy from the Government
Best Wallet Not 1st	-0.1301*** (0.0161)	-0.1761*** (0.0240)	-0.1320*** (0.0147)	-0.1839*** (0.0225)	-0.0379*** (0.0130)	-0.0164 (0.0165)
Increased Transparency	**-17%**	0.0902*** (0.0210)	**-46%**	-0.1845*** (0.0225)	**-32%**	0.0644*** (0.0231)
Best Not 1st × Increased Transparency		0.0966*** (0.0318)		0.1082*** (0.0290)		-0.0391 (0.0257)
Constant	0.7777*** (0.0105)	0.7313*** (0.0161)	0.2867*** (0.0115)	0.3779*** (0.0174)	0.1199*** (0.0117)	0.0859*** (0.0148)
Observations	3,108	3,108	3,108	3,108	3,108	3,108
R-squared	0.021	0.047	0.025	0.054	0.003	0.008

VARIABLES	(1) Maximized Privacy from the Public	(2) Maximized Privacy from the Public	(3) Maximized Privacy from the Intermediary	(4) Maximized Privacy from the Intermediary	(5) Maximized Privacy from the Government	(6) Maximized Privacy from the Government
Best Wallet Not 1st	-0.1301***	-0.1761***	-0.1320***	-0.1839***	-0.0379***	-0.0164
	(0.0161)	(0.0240)	(0.0147)	(0.0225)	(0.0130)	(0.0165)
Increased Transparency		0.0902***		-0.1845***		0.0644***
		(0.0210)		(0.0225)		(0.0231)
Best Not 1st × Increased Transparency		0.0966***		0.1082***		-0.0391
		(0.0318)		(0.0290)		(0.0257)
Constant	0.7777***	0.7313***	0.2867***	0.3779***	0.1199***	0.0859***
	(0.0105)	(0.0161)	(0.0115)	(0.0174)	(0.0117)	(0.0148)
Observations	3,108	3,108	3,108	3,108	3,108	3,108
R-squared	0.021	0.047	0.025	0.054	0.003	0.008

3. Small Talk

Can easily distract people from escaping surveillance with orthogonal talk…

Encryption Randomization

"PGP is a program that gives your electronic mail something that it otherwise doesn't have: Privacy. It does this by encrypting your mail so that nobody but the intended person can read it. When encrypted, the message looks like a meaningless jumble of random characters. PGP has proven itself quite capable of resisting even the most sophisticated forms of analysis aimed at reading the encrypted text.

PGP can also be used to apply a digital signature to a message without encrypting it. This is normally used in public postings where you don't want to hide what you are saying, but rather want to allow others to confirm that the message actually came from you. Once a digital signature is created, it is impossible for anyone to modify either the message or the signature without the modification being detected by PGP."

PGP makes sure that any communication between you and someone else can only be read by the sender and the receiver.

"End-to-end encryption creates a sort of digital tunnel between the senders and receivers of e-mails -- helping to keep the prying eyes of everyone from governments to Internet service providers and mail providers themselves from seeing the content of messages" (source: http://www.washingtonpost.com/blogs/the-switch/wp/2014/08/07/yahoo-to-role-out-end-to-end-encryption-option-for-all-yahoo-mail-users-in-2015/)

Although the technology has been available for a while, it is catching traction among those concerned about privacy and security. Both Yahoo! and Google have recently announced plans to integrate PGP into their email services. (For more information: http://en.wikipedia.org/wiki/Pretty_Good_Privacy)

Effect of Small Talk on Privacy

VARIABLES	(1) Escaping Surveillance from the Public	(2) Escaping Surveillance from the Intermediary	(3) Escaping Surveillance from the Government
Encryption Randomization	-0.0105* (0.0061)	-0.0361 (0.0250)	-0.0331* (0.0182)
Constant	0.0229*** (0.0049)	0.6921*** (0.0175)	0.8820*** (0.0122)
Observations	1,882	1,410	1,410
R-squared	0.002	0.001	0.002

PRIVACYCON

Conclusions (I)

- Although we study a very specific setting and technology…we are able to document possibly more general digital privacy paradoxes using **field experiment** data
  - People say they care about privacy, but in the face of **'small money'** they are willing to share very sensitive data
  - People say they want privacy-protecting technologies but are put off from using them by very **'small costs'** such as scrolling down a list
  - People worry about government surveillance, but stop worrying when receive reassurance **'small talk'** about something completely orthogonal

Conclusions (II)

- Debate in the US and Europe about the regulation of **personal data**
- Sensitive data is becoming more valuable because of **machine learning and prediction**
- Survey-based privacy research may not be best grounding for policy
- Policy focus has been on restricting data access through use of **consent mechanisms…**but this approach has implicit in it assumptions about the **lack of malleability** of users' preferences
- We document multiple, potential market failures in digital privacy

Thank you!

Christian Catalini
blockchain.mit.edu
catalini@mit.edu