The Economics of Privacy: An Agenda

Catherine Tucker

MIT Sloan and NBER
Challenges to Studying Privacy

The History of the Economics of Privacy

Outstanding Questions

Final Thoughts
Challenges to Studying Privacy
Modeling it is Hard
Bound Up in Technological Change
What is Privacy?

My Favorite Definition: Freedom from Unwarranted Intrusion
CAN PRIVACY BE JUST ANOTHER GOOD?

JOSEPH FARRELL*

I. PRIVACY AS FINAL GOOD AND INTERMEDIATE GOOD ............ 251
II. TREATING PRIVACY AS A FINAL GOOD WITH CONSUMER
    SOVEREIGNTY: INITIAL AGREEMENTS........................................... 253
    A. How Initial Agreements Can Work Well.............................. 254
    B. How Initial Agreements Can Fail...................................... 256
III. MODIFYING POLICIES LATER.................................................. 259
    A. Communication and Negotiation....................................... 260
    B. Direction of Payments and the Role of Content and
       Advertising......................................................................... 260
CONCLUSION.................................................................................. 261
Challenges to Studying Privacy
Modeling it is Hard
Bound Up in Technological Change
THE RIGHT TO PRIVACY.

"It could be done only on principles of private justice, moral fitness, and public convenience, which, when applied to a new subject, make common law without a precedent; much more when received and approved by usage."

WILLIS, J., in MILLER v. TAYLOR, 4 BUNCE, 1203, 1210.

...WHAT the individual shall have full protection in person and...
A Shift in Costs of Data Storage

- In 2001, 1 GB cost $19.70 to store.
- In 2010, 1 GB cost $0.06 to store.
- In 2022, 1 GB cost $0.0023/GB to store.
Your AI pair programmer

GitHub Copilot uses the OpenAI Codex to suggest code and entire functions in real-time, right from your editor.

Start my free trial  Explore docs
All These Mean That How We Model And Think About Privacy is Constantly Changing
Agenda

Challenges to Studying Privacy

The History of the Economics of Privacy

Outstanding Questions

Final Thoughts
The Economics of Privacy†

ALESSANDRO ACQUISTI, CURTIS TAYLOR, AND LIAD WAGMAN

This article summarizes and draws connections among diverse streams of theoretical and empirical research on the economics of privacy. We focus on the economic value and consequences of protecting and disclosing personal information, and on consumers’ understanding and decisions regarding the trade-offs associated with the privacy and the sharing of personal data. We highlight how the economic analysis of privacy evolved over time, as advancements in information technology raised increasingly nuanced and complex issues. We find and highlight three themes that connect diverse insights from the literature. First, characterizing a single unifying economic theory of privacy is hard, because privacy issues of economic relevance arise in widely diverse contexts. Second, there are theoretical and empirical situations where the protection of privacy can both enhance and detract from individual and societal welfare. Third, in digital economies, consumers’ ability to make informed decisions about their privacy is severely hindered because consumers are often in a position of imperfect or asymmetric information regarding when their data is collected, for what purposes, and with what consequences. We conclude the article by highlighting some of the ongoing issues in the privacy debate of interest to economists. (JEL D82, D83, G20, I10, L13, M31, M37)
And let me assure you are speakers today will more than justice to this...

<table>
<thead>
<tr>
<th>Time</th>
<th>Session Title</th>
<th>Speaker(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>9:00 am</td>
<td>Introductions</td>
<td></td>
</tr>
<tr>
<td>9:15 am</td>
<td>Introduction to the Economics of Privacy</td>
<td>Catherine Tucker, Massachusetts Institute of Technology and NBER</td>
</tr>
<tr>
<td>10:15 am</td>
<td>Break</td>
<td></td>
</tr>
<tr>
<td>10:30 am</td>
<td>Theory and Privacy (slides)</td>
<td>Alessandro Bonatti, Massachusetts Institute of Technology</td>
</tr>
<tr>
<td>11:30 am</td>
<td>Break</td>
<td></td>
</tr>
<tr>
<td>11:45 am</td>
<td>Privacy of Digital Health Information</td>
<td>Amalia R. Miller, University of Virginia and NBER</td>
</tr>
<tr>
<td>12:45 pm</td>
<td>Lunch - Room Longfellow A</td>
<td></td>
</tr>
<tr>
<td>1:45 pm</td>
<td>Empirical Economic Research on Privacy Regulation: Lessons from the GDPR and Beyond (slides)</td>
<td>Garrett Johnson, Boston University</td>
</tr>
<tr>
<td>2:45 pm</td>
<td>Break</td>
<td></td>
</tr>
<tr>
<td>3:00 pm</td>
<td>The Economics of Privacy at a Crossroads</td>
<td>Alessandro Acquisti, Carnegie Mellon University</td>
</tr>
<tr>
<td>4:00 pm</td>
<td>Future Directions (General Discussion)</td>
<td></td>
</tr>
</tbody>
</table>
So What Am I Going To Do?

Well I am a Marketing Professor....
Share Some Ideas About Good Research Topics for Junior Researchers

Not in any way intended to be exhaustive.
Agenda

Challenges to Studying Privacy

The History of the Economics of Privacy

Outstanding Questions

Final Thoughts
Outstanding Questions
The Value of Privacy
  Let’s Measure Some Benefits to Privacy Regulation
  Measuring Privacy Preferences
  Privacy Preferences and Contextual Integrity
  Privacy Preferences and Information Security Concerns
  Time-Inconsistency in Privacy Preferences
Markets and Privacy
The Spread of Privacy Protective Technologies
Algorithmic Privacy
The Broader Economy and Privacy
Outstanding Questions

The Value of Privacy

Let’s Measure Some Benefits to Privacy Regulation
- Measuring Privacy Preferences
- Privacy Preferences and Contextual Integrity
- Privacy Preferences and Information Security Concerns
- Time-Inconsistency in Privacy Preferences

Markets and Privacy

The Spread of Privacy Protective Technologies

Algorithmic Privacy

The Broader Economy and Privacy
I am completely guilty of this

Privacy and Innovation

Avi Goldfarb and Catherine Tucker
Rotman School of Management, University of Toronto; MIT Sloan School of Management and NBER

Abstract

Information and communication technologies now enable firms to collect detailed and potentially intrusive data about their customers both easily and cheaply. Privacy concerns are thus no longer limited to government surveillance and public figures’ private lives. The empirical literature shows that privacy regulation may affect the extent and direction of data-based innovation. We also show that the impacts of privacy regulation can be extremely heterogeneous. We therefore argue that digitization has made privacy policy a part of innovation policy.
Privacy Regulation Might Halt The Spread of Data Associated With Unfounded Stigma

- Mental Health
- Reproductive Health
- Past Crimes
Privacy Regulation Might Halt The Spread of Data Associated With Addiction

- Health
- Spending
- Gambling
But if we want to measure more global benefits to privacy regulation we need to model consumer tastes for privacy better.
Breakdown

Outstanding Questions

The Value of Privacy
- Let’s Measure Some Benefits to Privacy Regulation
- Measuring Privacy Preferences
- Privacy Preferences and Contextual Integrity
- Privacy Preferences and Information Security Concerns
- Time-Inconsistency in Privacy Preferences

Markets and Privacy
- The Spread of Privacy Protective Technologies

Algorithmic Privacy
- The Broader Economy and Privacy
So Far

Valuing Intrinsic and Instrumental Preferences for Privacy

Tesary Lin

Published Online: 13 May 2022 | https://doi.org/10.1287/mksc.2022.1368

Abstract

I empirically separate two components in a consumer's privacy preference. The intrinsic component is a “taste” for privacy, a utility primitive. The instrumental component comes from the consumer's anticipated economic loss from revealing his private information to the firm and arises endogenously from a firm's usage of consumer data. Combining an experiment and a structural model, I measure the revealed preferences separately for each component. Intrinsic preferences have seemingly small mean values, ranging from $0.14 to $2.37 per demographic variable. Meanwhile, they are highly heterogeneous across consumers and categories of data: The valuations of consumers at the right tail often exceed the firm's valuation of consumer data. Consumers’ self-selection into data sharing depends on the respective magnitudes and correlation between the two preference components and often deviates from the “low types are more willing to hide” argument. Through counterfactual analysis, I show how this more nuanced selection pattern changes a firm’s inference from consumers’ privacy decisions and its data-buying strategy.
And Also

What This Tells Me We Need

Papers with individual-level privacy choice data over time across difference dimensions. Without that it is hard to make much progress given our current tool kit. (But even this would suffer truncation)
Outstanding Questions

The Value of Privacy
- Let’s Measure Some Benefits to Privacy Regulation
- Measuring Privacy Preferences
- Privacy Preferences and Contextual Integrity
- Privacy Preferences and Information Security Concerns
- Time-Inconsistency in Privacy Preferences

Markets and Privacy
- The Spread of Privacy Protective Technologies

Algorithmic Privacy
- The Broader Economy and Privacy
The Theory of Contextual Integrity May Give Us Insights into How To Model Heterogeneity of Privacy Preferences Across Domains, Times and Individuals
Contextual Integrity Theory: Helen Nissenbaum

PARAMETERS
- Actors
  - Physician, merchant, bank, friend, merchant, police,
  - Verizon, shopper, investor, reader, advertiser, voter,
  - insurance company, parent, spouse, teacher, friend,
  - student, FBI, CIA, neighbor

- Information types
  - Demographic, biographical, transactional, what you
  - read, movies you’ve seen, metadata, purchases,
  - salary, address, medical diagnosis, facial image, SSN,
  - how much you paid for your house, grades, spoons of
  - sugar in your coffee, sexual orientation

- Transmission Principles
  - Consent, coerce, compel, steal, buy, sell, in confidence,
  - surreptitiously, with notice, with a warrant, with
  - authorization, reciprocal, as required by law

The IACR. (2019, October 4). International Association for Cryptologic Research, Invited talk: Contextual Integrity. YouTube. https://www.youtube.com/watch?v=aVRbtxVGDc
Outstanding Questions
The Value of Privacy
  Let’s Measure Some Benefits to Privacy Regulation
  Measuring Privacy Preferences
  Privacy Preferences and Contextual Integrity
  Privacy Preferences and Information Security Concerns
  Time-Inconsistency in Privacy Preferences
Markets and Privacy
The Spread of Privacy Protective Technologies
Algorithmic Privacy
The Broader Economy and Privacy
Can This Framework Help Us Distinguish Between Information Security and Privacy Concerns?
Outstanding Questions

The Value of Privacy
- Let’s Measure Some Benefits to Privacy Regulation
- Measuring Privacy Preferences
- Privacy Preferences and Contextual Integrity
- Privacy Preferences and Information Security Concerns
- Time-Inconsistency in Privacy Preferences

Markets and Privacy
- The Spread of Privacy Protective Technologies

Algorithmic Privacy
- The Broader Economy and Privacy
Shifts in Privacy Concerns†

By Avi Goldfarb and Catherine Tucker*
Figure 1. Fraction Refusing to Reveal Income by Age and Year
Inferences From Data Created In Your Youth
Outstanding Questions
  The Value of Privacy
Markets and Privacy
  Property Rights and Privacy
  Individual Data Markets
  Competitive Dynamics and Privacy
The Spread of Privacy Protective Technologies
Algorithmic Privacy
The Broader Economy and Privacy
Outstanding Questions

- The Value of Privacy

Markets and Privacy

- Property Rights and Privacy
- Individual Data Markets
- Competitive Dynamics and Privacy

The Spread of Privacy Protective Technologies

Algorithmic Privacy

The Broader Economy and Privacy
All Economists When Asked to Comment on Privacy
But are Property Rights Easy to Define?

- Beyond Binary Data
- Spillovers
- Inferences Rather than Data
Breakdown

Outstanding Questions
The Value of Privacy

Markets and Privacy
Property Rights and Privacy
Individual Data Markets
Competitive Dynamics and Privacy

The Spread of Privacy Protective Technologies
Algorithmic Privacy
The Broader Economy and Privacy
Why haven’t Individual Data Markets worked?

How It Works

We reward people like you for helping us improve the Internet. Become part of our research community of over 2 million members today and start earning rewards!

Here’s what you’ll need to do:

- Install our software on your mobile device
- Claim your earned credits each week
- Redeem those credits for eGift cards
One obvious explanation is asymmetric information and moral hazard
Another explanation is that data is just very cheap.
<table>
<thead>
<tr>
<th>Breakdown</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Outstanding Questions</strong></td>
</tr>
<tr>
<td>- The Value of Privacy</td>
</tr>
<tr>
<td><strong>Markets and Privacy</strong></td>
</tr>
<tr>
<td>- Property Rights and Privacy</td>
</tr>
<tr>
<td>- Individual Data Markets</td>
</tr>
<tr>
<td>- Competitive Dynamics and Privacy</td>
</tr>
<tr>
<td><strong>The Spread of Privacy Protective Technologies</strong></td>
</tr>
<tr>
<td><strong>Algorithmic Privacy</strong></td>
</tr>
<tr>
<td><strong>The Broader Economy and Privacy</strong></td>
</tr>
</tbody>
</table>
Privacy & Market Concentration: Intended & Unintended Consequences of the GDPR

57 Pages  •  Posted: 15 Nov 2019  •  Last revised: 22 Sep 2022

Garrett Johnson
Questrom School of Business

Scott Shriver
University of Colorado at Boulder - Department of Marketing

Samuel Goldberg
Stanford Institute for Economic Policy Research

Date Written: September 21, 2022

Abstract
We show that websites' vendor use falls after the European Union’s General Data Protection Regulation (GDPR), but that market concentration also increases among technology vendors that provide support services to websites. We collect panel data on the web technology vendors selected by more than 27,000 top websites internationally. The week after the GDPR’s enforcement, website use of web technology vendors falls by 15% for EU residents. Websites are relatively more likely to retain top vendors, which increases the concentration of the vendor market by 17%. Increased concentration predominantly arises among vendors that use personal data such as cookies, and from the increased relative shares of Facebook and Google-owned vendors, but not from website consent requests. Though the aggregate changes in vendor use and vendor concentration dissipate by the end of 2018, we find that the GDPR impact persists in the advertising vendor category most scrutinized by regulators. Our findings shed light on potential explanations for the sudden drop and subsequent rebound in vendor usage.

Keywords: Privacy, GDPR, Competition, Web Technology, Regulatory compliance

JEL Classification: D04, K21, L11, L22, L51, L86, M30, M38, O38

Suggested Citation:
Let's Look at the Dynamics Elsewhere

Global EdTech and Smart Classrooms Market Report 2022-2027 Featuring Leading Players - Apple, Cisco, Blackboard, IBM, Dell EMC, Google, Microsoft, Oracle, SAP, & Instructure - ResearchAndMarkets.com

August 04, 2022 08:37 AM Eastern Daylight Time

The "Global EdTech and Smart Classrooms Market by Hardware (Interactive Displays, Interactive Projectors), Education System Solution (LMS, TMS, DMS, SRS, Test Preparation, Learning & Gamification), Deployment Type, End User and Region - Forecast to 2027" report has been added to ResearchAndMarkets.com's offering.

The publisher forecasts the global EdTech and smart classrooms market to grow from USD 125.3 billion in 2022 to USD 232.9 billion by 2027, at a Compound Annual Growth Rate (CAGR) of 13.2%.

The major factors driving the growth of the EdTech and smart classrooms market include growing adoption of eLearning solutions, impact of COVID-19 pandemic and growing need for online teaching-learning models to continue education system in lockdown.
In Depth

Outstanding Questions

The Value of Privacy
Markets and Privacy

The Spread of Privacy Protective Technologies

The Diffusion of Privacy Protective Technologies
Do Privacy Protective Technologies Actually Enhance Welfare?
Cryptoeconomics and Privacy

Algorithmic Privacy

The Broader Economy and Privacy
Outstanding Questions

The Value of Privacy
Markets and Privacy

The Spread of Privacy Protective Technologies
The Diffusion of Privacy Protective Technologies
Do Privacy Protective Technologies Actually Enhance Welfare?
Cryptoeconomics and Privacy

Algorithmic Privacy

The Broader Economy and Privacy
Let's Move Beyond Studies of Ad Blocking and Move to the Firm

Product Category Descriptions

Privacy program management – solutions designed specifically for the privacy office.

Assessment managers tend to automate different functions of a privacy program, such as operationalizing privacy impact assessments, locating risk gaps, demonstrating compliance and helping privacy officers scale complex tasks requiring spreadsheets, data entry and reporting.

Consent managers help organizations collect, track, demonstrate and manage users’ consent.

Data mapping solutions can come in manual or automated form and help organizations determine data flows throughout the enterprise.

Data subject request solutions help organizations facilitate inquiries made by individuals who wish to exercise their data rights. These can include requests involving the right to access, rectification, portability and erasure.

Incident response solutions help companies respond to a data breach incident by providing information to relevant stakeholders of what was compromised and what notification obligations must be met.

Privacy information managers provide organizations with extensive and often automated information on the latest privacy laws around the world.

Website scanning is a service that primarily checks a client’s website to determine what cookies, beacons and other trackers are embedded to help protect the client’s privacy.
Breakdown

Outstanding Questions
  The Value of Privacy
  Markets and Privacy
  The Spread of Privacy Protective Technologies
    The Diffusion of Privacy Protective Technologies
    Do Privacy Protective Technologies Actually Enhance Welfare?
  Cryptoeconomics and Privacy
  Algorithmic Privacy
  The Broader Economy and Privacy
Costs of Regulation or Privacy Enhancing?

2022 Privacy Tech VENDOR REPORT

By IAPP Staff Writer Alex LaCasse

The IAPP presents its sixth annual “Privacy Tech Vendor Report.” In previous editions, the report examined the growth and trends of the privacy technology marketplace year over year. This issue, the IAPP lists 364 privacy technology vendors, each featured in the directory section of this report.

In the last six years, privacy tech has become a critical industry offering solutions for an ever-evolving global regulatory system that places a greater emphasis on user privacy. A key takeaway is that while the privacy tech industry has grown exponentially, it stands on the precipice of a fundamental sea change, facing possible consolidation and specialization geared toward specific customer solutions.

This year’s “Privacy Tech Vendor Report” finds the industry at a crossroads of sorts. As privacy has shifted from an afterthought to a necessity within the last decade, the conversation today regarding its place in product development has evolved from the abstract to the technical implementation of an array of solutions.

“Companies are now moving toward understanding what their privacy tech requirements are, and I can’t say enough about how that was just not a thing, even a few years ago.”

Chief Strategy Officer Mark Thompson, CIPP/E, CIPM, CIPT, FIP, “For the vendors that have ‘got it right,’ there is a clear opportunity to differentiate from the pack by showing an enhanced understanding of customer needs and how their products help solve these challenges.”

Astrachain co-founder and CEO Yosra Jarraha said the privacy tech marketplace has grown past the point of solely playing catch-up with the implementation and enforcement of privacy laws around the world. Instead, it now looks to build comprehensive technical solutions to big-picture data security concerns.
Outstanding Questions

The Value of Privacy
Markets and Privacy
The Spread of Privacy Protective Technologies
  The Diffusion of Privacy Protective Technologies
  Do Privacy Protective Technologies Actually Enhance Welfare?
  Cryptoeconomics and Privacy
Algorithmic Privacy
The Broader Economy and Privacy
Cryptoeconomy: NFTs could be the way to data privacy

"Anything that you post on the internet isn't yours anymore." A lot of us who grew up in the age of the internet heard that a lot because it's virtually true. Once you post something online, any and everybody can download it, manipulate it and you have no control over it. However, this might be changing with the introduction of NFTs as the next resource for digital identity management and data privacy.
In Depth

Outstanding Questions
- The Value of Privacy
- Markets and Privacy
- The Spread of Privacy Protective Technologies

Algorithmic Privacy
- Inferential Privacy
- Privacy and Algorithmic Discrimination
- The Broader Economy and Privacy
Breakdown

**Outstanding Questions**
- The Value of Privacy
- Markets and Privacy
- The Spread of Privacy Protective Technologies
- **Algorithmic Privacy**
  - Inferential Privacy
  - Privacy and Algorithmic Discrimination
- The Broader Economy and Privacy
Private traits and attributes are predictable from digital records of human behavior

Michal Kosinski1, David Stillwell2, and Thore Graepel3

1Free School Lane, The Psychometrics Centre, University of Cambridge, Cambridge CB2 3RQ United Kingdom; and 3Microsoft Research, Cambridge CB1 2FB, United Kingdom

Edited by Kenneth Wachter, University of California, Berkeley, CA, and approved February 12, 2013 (received for review October 29, 2012)

We show that easily accessible digital records of behavior, Facebook Likes, can be used to automatically and accurately predict a range of highly sensitive personal attributes including: sexual orientation, ethnicity, religious and political views, personality traits, intelligence, happiness, use of addictive substances, parental separation, age, and gender. The analysis presented is based on a dataset of over 58,000 volunteers who provided their Facebook Likes, detailed demographic profiles, and the results of several psychometric tests. The proposed model uses dimensionality reduction for preprocessing the Likes data, which are then entered into logistic/linear regression to predict individual psychodemographic profiles from Likes. The model correctly discriminates between homosexual and heterosexual men in 88% of cases, African Americans and Caucasian Americans in 95% of cases, and between Democrat and Republican in 85% of cases. For the personality trait “Openness,” prediction accuracy is close to the test-retest accuracy of a standard personality test. We give examples of associations between attributes and Likes and discuss implications for online personalization and privacy.

browsing logs (11–15). Similarly, it has been shown that personality can be predicted based on the contents of personal Web sites (16), music collections (17), properties of Facebook or Twitter profiles such as the number of friends or the density of friendship networks (18–21), or language used by their users (22). Furthermore, location within a friendship network at Facebook was shown to be predictive of sexual orientation (23).

This study demonstrates the degree to which relatively basic digital records of human behavior can be used to automatically and accurately estimate a wide range of personal attributes that people would typically assume to be private. The study is based on Facebook Likes, a mechanism used by Facebook users to express their positive association with (or “Like”) online content, such as photos, friends’ status updates, Facebook pages of products, sports, musicians, books, restaurants, or popular Web sites. Likes represent a very generic class of digital records, similar to Web search queries, Web browsing histories, and credit card purchases. For example, observing users’ Likes related to music provides similar information to observing records of songs listened to online, songs and artists searched for using a Web search engine, or subscriptions to related Twitter channels. In contrast to these other sources of information, Facebook Likes are unusual in that they are currently publicly available by default. However,
Inferential Privacy Makes Real The Question of The Unpredictability of Algorithmic Progress
Outstanding Questions
The Value of Privacy
Markets and Privacy
The Spread of Privacy Protective Technologies
Algorithmic Privacy
Inferential Privacy
Privacy and Algorithmic Discrimination
The Broader Economy and Privacy
The debate on privacy harms has moved on to algorithmic discrimination.
FEDERAL TRADE COMMISSION

16 CFR Part 464

Trade Regulation Rule on Commercial Surveillance and Data Security

AGENCY: Federal Trade Commission.

ACTION: Advance notice of proposed rulemaking; request for public comment; public forum.

SUMMARY: The Federal Trade Commission (“FTC”) is publishing this advance notice of proposed rulemaking (“ANPR”) to request public comment on the prevalence of commercial surveillance and data security practices that harm consumers. Specifically, the Commission invites comment on whether it should implement new trade regulation rules or other regulatory alternatives concerning the ways in which companies (1) collect, aggregate, protect, use, analyze, and retain consumer data, as well as (2) transfer, share, sell, or otherwise monetize that data in ways that are unfair or deceptive.
Outstanding Questions

- The Value of Privacy
- Markets and Privacy
- The Spread of Privacy Protective Technologies
- Algorithmic Privacy

The Broader Economy and Privacy

- Privacy and Inequality
- The Political Economy of Government Surveillance
- Privacy and Trade
Outstanding Questions
- The Value of Privacy
- Markets and Privacy
- The Spread of Privacy Protective Technologies
- Algorithmic Privacy
- The Broader Economy and Privacy
  - Privacy and Inequality
  - The Political Economy of Government Surveillance
- Privacy and Trade
Technology

Amazon to Bring Same-Day Delivery to Roxbury After Outcry

- Largely black Boston neighborhood was excluded from service
- Illinois Congressman wants FTC to investigate delivery areas

By Spencer Soper
April 26, 2016 at 5:49 PM EDT  Updated on April 26, 2016 at 8:22 PM EDT
The Mirror of Privacy Policy: Data Deserts
Outstanding Questions

The Value of Privacy
Markets and Privacy
The Spread of Privacy Protective Technologies
Algorithmic Privacy

The Broader Economy and Privacy

Privacy and Inequality

The Political Economy of Government Surveillance
Privacy and Trade
AI-tocracy
Martin Beraja, Andrew Kao, David Y. Yang, and Noam Yuchtman
NBER Working Paper No. 29466
November 2021
JEL No. E00,L5,L63,O25,O30,O40,P00

ABSTRACT

Can frontier innovation be sustained under autocracy? We argue that innovation and autocracy can be mutually reinforcing when: (i) the new technology bolsters the autocrat’s power; and (ii) the autocrat’s demand for the technology stimulates further innovation in applications beyond those benefiting it directly. We test for such a mutually reinforcing relationship in the context of facial recognition AI in China. To do so, we gather comprehensive data on AI firms and government procurement contracts, as well as on social unrest across China during the last decade. We first show that autocrats benefit from AI: local unrest leads to greater government procurement of facial recognition AI, and increased AI procurement suppresses subsequent unrest. We then show that AI innovation benefits from autocrats’ suppression of unrest: the contracted AI firms innovate more both for the government and commercial markets. Taken together, these results suggest the possibility of sustained AI innovation under the Chinese regime: AI innovation entrenches the regime, and the regime’s investment in AI for political control stimulates further frontier innovation.
Government Surveillance and Internet Search Behavior

Alex Matthews
Digital Fourth / Restore The Fourth

Catherine E. Tucker
Massachusetts Institute of Technology (MIT) - Management Science (MS)

Date Written: February 17, 2017

Abstract
This paper displays data from the US and its top 40 trading partners on the search volume of select keywords from before and after the surveillance revelations of June 2013, to analyze whether Google users' search behavior changed as a result. The surveillance revelations are treated as an exogenous shock in information about how closely users' internet searches were being monitored by the US government. Each search term was independently rated for its degree of privacy sensitivity along multiple dimensions. Using panel data, our results suggest that search terms that were deemed both personally-sensitive and government-sensitive were most negatively affected by the PRISM revelations, highlighting the interplay between privacy concerns relating to both the government and the private individual. Perhaps surprisingly, the largest 'chilling effects' were not found in countries conventionally treated as intelligence targets by the US, but instead in countries that were more likely to be considered allies of the US. We show that this was driven in part by a fall in searches on health-related terms. Suppressing health information searches potentially harms the health of search engine users and, by reducing traffic on easy-to-monetize queries, also harms search engines’ bottom line. In general, our results suggest that there is a chilling effect on search behavior from government surveillance on the Internet, and that government surveillance programs may damage the profitability of US-based internet firms relative to non-US-based internet firms.

Keywords: surveillance, Snowden, prism, chilling effects, international trade
Breakdown

Outstanding Questions
  The Value of Privacy
  Markets and Privacy
  The Spread of Privacy Protective Technologies
  Algorithmic Privacy

The Broader Economy and Privacy
  Privacy and Inequality
  The Political Economy of Government Surveillance
  Privacy and Trade
F.C.C. Readies Vote on Banning New Huawei and ZTE Devices

The vote, which is expected to pass, is required by a law that President Biden signed last year.

Jessica Rosenworcel, the F.C.C. chairwoman, said the agency “remains committed to protecting our national security by ensuring that untrustworthy communications equipment is not authorized for use within our borders.” Foo photo by Jonathan Newton.

By David McCabe and Cecilia Kang
Oct. 13, 2022  Updated 2:33 p.m. ET
Biden hopes privacy appeals for EU citizens will save data flows

The president is signing an order implementing the details of an agreement with the EU to replace Privacy Shield.
<table>
<thead>
<tr>
<th>Agenda</th>
</tr>
</thead>
<tbody>
<tr>
<td>Challenges to Studying Privacy</td>
</tr>
<tr>
<td>The History of the Economics of Privacy</td>
</tr>
<tr>
<td>Outstanding Questions</td>
</tr>
<tr>
<td>Final Thoughts</td>
</tr>
</tbody>
</table>
If I get to this final slide in an hour I literally won’t believe it

But thank you a lot for listening and can’t wait for your thoughts and ideas about where the field should go
cetucker@mit.edu