Chitra Marti

chitramarti.com
chitra.marti@nyu.edu ● +1 (212) 998-0877

EDUCATION

New York University, Stern School of Business Sep 2019 – Jun 2024 (Expected)

PhD Candidate, Economics
Fields: Industrial Organization and Macroeconomics
Advisors: Christopher Conlon and Hanna Halaburda
Dissertation Title: Competition and Cybercrime

Princeton University Sep 2013 – Jun 2017

A.B. Economics, *Magna Cum Laude*
Certificates (Minors): Computer Science, Statistics & Machine Learning
Thesis: Planned Obsolescence: Examining Dynamic Consumer Preferences for Durability and Novelty (advised by Jakub Kastl)

HONORS AND FELLOWSHIPS

National Science Foundation Graduate Research Fellowship, Honorable Mention Mar 2021

Statistics & Machine Learning Independent Work Prize, Princeton University Jun 2017
Awarded for my junior paper, "Credibility and Conformity: The Effect of the Yelp Elite" for "exciting applications of statistics and machine learning methods."

WORKS IN PROGRESS

"Competition and Cybercrime: an Empirical Application Electronic Medical Records Firms"

"Overphishing: Competitive Cybercriminals and Vulnerability Disclosure"

"Are Firms Overvaluing Data? Evidence from 13,000 Android Apps" (with Raveesh Mayya)

"Blockchain Governance and Security" (with Noa Bar-Nir, Neil Gandal, Hanna Halaburda, and David Salant)

PUBLICATIONS

"Why is Inflation Low Globally?" with Òscar Jordà, Fernanda Nechio, and Eric Tallman. *FRBSF Economic Letter*. *FRBSF Economic Letter* 2019-19.
"Inflation: Stress-Testing the Phillips Curve" with Òscar Jordà, Fernanda Nechio, and Eric Tallman. 2019. *FRBSF Economic Letter* 2019-05.
"Does Ultra-Low Unemployment Spur Rapid Wage Growth?" with Sylvain Leduc and Dan Wilson. 2019. *FRBSF Economic Letter* 2019-02.
"Credibility and Conformity: The Effect of the Yelp Elite", *Princeton Undergraduate Research Journal*, Fall 2017 Issue.

SEMINARS AND INVITED CONFERENCES

2023: NBER Digitization Tutorial, New York University (Applied Micro, Industrial Organization)
2022: New York University (Micro Theory, Applied Micro, Industrial Organization), NBER Digitization Tutorial, Workshop on the Economics of Information Security (Lightning Round), NBER Entrepreneurship Boot Camp, NBER Economics of Privacy Tutorial
2021: New York University (Applied Micro), Boston University WEorg Workshop
2019: Western Economic Association Conference (two separate sessions), Federal Reserve Bank of Cleveland

TEACHING EXPERIENCE

Microeconomics with Calculus, Undergraduate 2022 (Spring, Summer, Fall), 2023 (Spring)

Firms and Markets, MBA Program Summer 2021

Introduction to Macroeconomics, Business and Political Economy Program Spring 2021

PROFESSIONAL SERVICE & PUBLIC GOODS

Referee for *Management Science*
Organizer and Mentor, Federal Reserve Research Associate Conference
Local Projections for Stata

RESEARCH EXPERIENCE

New York University Department of Economics New York, NY — Jan 2020 – Present
Research Assistant for Sylvain Chassang, Chris Conlon, and Raluca Ursu

Federal Reserve Bank of San Francisco San Francisco, CA — Jul 2017 – Jul 2019
Head Research Associate, Macroeconomics

Princeton University Department of Economics Princeton, NJ — Mar 2015 – Jun 2017
Research Assistant for Sylvain Chassang and Ilyana Kuziemko

U.S. Securities and Exchange Commission Washington, D.C. — May 2014 – Aug 2014
Research Intern in the Office of Markets, Division of Economic Risk and Analysis

OTHER PROFESSIONAL EXPERIENCE

Citigroup Global Markets Inc. New York, NY — May 2016 – Aug 2016
Summer Analyst in Global New Products, Capital Markets Origination

Princeton University Writing Center Princeton, NJ — Sep 2014 – Jun 2017
Writing Center Fellow and Independent Research & Thesis Mentor

REFERENCES

Prof. Christopher Conlon
Associate Professor of Economics, New York University, Stern School of Business
cconlon@stern.nyu.edu

Prof. Hanna Halaburda
Associate Professor of Technology, Operations, and Statistics, New York University, Stern School of Business
hh66@stern.nyu.edu

Prof. Luís Cabral
Paganelli-Bull Professor of Economics and International Business, New York University, Stern School of Business
luis.cabral@nyu.edu

Prof. Raveesh Mayya
Assistant Professor of Technology, Operations, and Statistics, New York University, Stern School of Business
raveesh@stern.nyu.edu

Chitra Marti
Application: Digital Economics and Artificial Intelligence Tutorial, Fall 2023
May 2, 2023 **Description of Research Interests and Projects:**

My research focuses on the risks and rewards of an increasingly digitized and networked world, with a focus on cybercrime.

The study of the economics of cybercrime rests at the intersection of the study of the **economics of digitization** (low costs of replication and scale, the death of distance) and the **economics of crime** (strategic criminal agents weighing costs and benefits). I approach the study of cybercrime from the perspective of an industrial organization economist, specifically thinking about how competitive forces among the defense (institutions, firms, and individuals) and the offense (between attackers) affect overall cybersecurity outcomes.

I have one primary project for which I would like advice, and would be grateful for the opportunity to learn more about what other researchers consider the most pressing questions in the field of digitization and strategy.

Competition and Cybercrime: an Application to Electronic Medical Records (*primary*) Cybercrime is pervasive on digital technologies and platforms, and threatens the sustainability of digital technologies for future use. Digital crime differs from physical crime in two key ways: first, attacks scale unlike any physical crime, with the marginal cost of attack decreasing as long as a common vector can be exploited. Second, attackers are strategic in choosing their targets, exploiting market concentration and supply chain structures to maximize payoff. A lack of jurisdiction and the "death of distance" via technology, the actual malicious attackers who exploit vulnerabilities to breach data or defraud users are rarely held accountable. Instead, then, policy has focused on how to encourage users and firms to properly defend themselves against the possibility of an attack.

The objective of the research is to construct a structural model of a market that may be subject to cyberattacks. Using data and an application to hospital data breaches of Electronic Health Records, I will be able to compare the effect of different policies on cybersecurity and consumer welfare. Some of the policies I consider are:

1. Mandated minimum security requirements (the most common and least controversial policy)
2. Firm-level supply chain requirements (implemented by a few large technology firms recently)
3. Antitrust policies that reduce the market power of large firms

I begin with a generalized theoretical model of a zero-sum game between attackers and users with threat and security investments. Technology firms provide data storage to users who have heterogeneous valuations for the service. The firms invest in security to protect themselves and their users. Users can then invest in additional protection. The firms experience economies of scale, and so is a natural monopolist. A strategic attacker, however, makes investments in breaching the firm and capturing value from its users. I model both sophisticated and unsophisticated consumers who consider both security and prices or just prices respectively when selecting a firm. The attacker experiences economies of scale in the number of users it can capture from a single firm.

The model elucidates five primary forces that drive the efficiency – both in terms of security and in total surplus – of any given market structure: (a) the natural monopoly structure maximizes the negative security externality the firm poses on users, and the concentration of value under one firm provides a lucrative target for the attacker; (b) assigning large liabilities to the firm can correct the externality and even encourage it to act as a "gatekeeper" to many users, reversing the previous force; (c) the ability of consumers to additionally protect themselves on top of the firm results in a "sum-of-efforts" style game between users and attackers, which encourages concentration but also facilitates free-riding by low-value consumers; (d) the attacker's economies of scale mean additional users of the service decrease the average cost of attack (a user-level externality that cannot be corrected with Coase Theorem transfers); and (e) price competition limits the incentive and ability of the firms to secure themselves properly.

I then apply the insights of the model empirically to data breaches of electronic medical records (EMRs). EMRs are the digitization of healthcare information. In 2009, the American Recovery and Reinvestment Act incentivized doctors and healthcare networks to adopt electronic medical records, leading to near-ubiquity. EMRs serve two purposes: to make data easily accessible to a wide variety of healthcare providers and patients, and to secure the data from malicious attackers. Malicious attackers value EMRs because healthcare data cannot be easily changed (unlike a credit card number), and typically pairs health information with insurance information and other personally identifiable information useful for blackmail, follow-on attacks, or insurance fraud.

A variety of firms compete to provider EMR mangement software to healthcare providers. The market is highly concentrated, with three firms claiming about 75% of the market (KLAS). EMR firms also regionally specialize, reducing further industry competition. How does competition affect the incentives to create a secure product, especially when it is not the firm but the user (hospital) who faces the cost of failure? How do the presence of economies of scale and endogenously strategic attackers complicate incentives?

The healthcare sector is unique because of its historical mandate that any breach of more than 500 records must be disclosed publicly. The data from the U.S. Department of Health and Human Services, thus has the universe of attacks that [have been known to] affect more than 500 individual records. The data classify the breach type (e.g. Hacking/IT vs. Physical Damage) and contain the institution breached, but not the mode. Over 5000 breaches have been reported in the last ten years, with the worst (Anthem Inc., 2015) affecting over 70 *million* patients. Breaches are linked to particular hospitals, with a description reporting whether fault might lie with the EMR firm (e.g. a software flaw) or not (e.g. a stolen laptop).

Data on vulnerabilities – the loopholes through which attackers enter – is publicly available in the Common Vulnerabilities and Exposures database. The CVE data provides a list of vulnerabilities – along with an exploitability score and a general description – for every publicly known (disclosed) vulnerability in any kind of software product. The data cover many EMR firms and the vulnerabilities in their product. Data on when software patches and updates are released to close vulnerabilities is available via individual firms' websites.

Finally, data matching the hospital to its EMR provider comes from two sources. The American Hospital Association's annual survey matches hospitals to their EMR provider from 2009 onwards, allowing me to track switches over time. It also contains an IT supplement describing a hospital's additional cyber-investment and preferences (how doctors are trained in EMRs, the number of IT staff, etc.).

The last dataset comes from Mordor Intelligence, a market research and consulting firm which

has microdata on provider-level choices of electronic medical records firms and the specific products chosen for about 100 of the largest hospitals. The data contain prices and product descriptions – particularly whether a hospital's EMR product is On-Premises or Cloud-Based, a distinction that affects the potential attack vector and quality.

The data above give me nearly every American *hospital* and its characteristics; any *data breaches* it experienced; whether their *EMR firm* was responsible; and the price, quality, and security properties of their EMR management software. I then can use typical demand estimation techniques to learn how much hospitals are willing to pay for security, and other product characteristics within each category. In particular, I can use a description of the product's quality and security to determine how consumers perceive the safety of their EMR products and trade off security with price. High levels of consumer price sensitivity, for example, would indicate that consumers value security relatively less, disincentivizing firm investment and push the market towards cheaper, worse providers. A structural model allows me to test how the policies described above to change security outcomes and hospital welfare.