TABLE OF CONTENTS

Executive Summary ........................................................................................................ 2

Goals and Strategy ........................................................................................................ 3

Key Project Developments .......................................................................................... 4

  1. Research Developments ....................................................................................... 4
  2. Education Developments ..................................................................................... 8

Collaboration ................................................................................................................ 11

Communication and Outreach ..................................................................................... 12

Impact ............................................................................................................................ 14

Appendix 1: Funded Research Project Descriptions .................................................. 16

Appendix 2: Cyber Initiative Seminars and Events .................................................... 28
Executive Summary

As of December 2016, the Stanford Cyber Initiative has concluded its second year of operations. The mission of the Cyber Initiative is to produce multi-disciplinary research and frame policy debates on the future of cyber-social systems, and the Initiative has been successful over the past two years in pursuing this mission. The Initiative has generated broad interest, engagement, cross-disciplinary collaboration and partnerships in the study of cyber-social systems across Stanford. This Report provides details of the various research, education and outreach activities that have been supported in various ways by the Initiative in the past year.

As described below, the Stanford Cyber Initiative has supported research activity and framed discussions about cyber-social systems by Stanford faculty and researchers, Stanford students, policy-makers, industry leaders, and a wide-ranging community that reads and listens to the Cyber Initiative’s publications and communication efforts. The Initiative has successfully engaged Stanford scholars across a wide range of disciplines, prompted them to study the ways in which cyber technologies has transformed the systems that they study, and encouraged them to build collaborations across disciplines that they had not previously attempted. The Initiative has built partnerships and collaborations with related centers across campus, and is now recognized as a leading hub at Stanford for the study of cyber issues and policy in a broad sense. As the Initiative begins its third year, it has begun to direct more emphasis toward two areas of great policy consequence: (a) the future of the digital economy and (b) the security risks of cyber-reliant systems.

This Report follows the structure of the Hewlett Foundation’s Interim Report Guidelines, as provided to us by Eli Sugarman. In accordance with the categories of information enumerated in these Guidelines, the sections of this report are “Goals and Strategy”, “Organizational Structure”, “Key Project Developments”, “Collaboration”, “Communication and Outreach”, “Impact”, “Obstacles and Risks”, and “Sustainability and Funding”. 
Goals and Strategy

Stanford’s grant proposal to the Foundation in 2014 identified three aims for the Stanford Cyber Initiative: “The first is advancing our understanding of the technical and societal aspects of cyber trust and trustworthiness, broadly defined. The second will focus on governance, values, and the public interest in relation to cyberspace. The third will explore the emergence of unexpected characteristics of cyberspace and the potential consequences for individuals, societies, markets, and institutions.” Consistent with these aims, the mission of the Initiative is to produce multi-disciplinary research and frame policy debates on the future of cyber-social systems.

The development and spread of digital technologies have transformed most of our social systems (our markets, workplace, transportation, education, democracy, etc.), into the various corresponding cyber-social systems in which humans interact. The Initiative adopted this concept of cyber-social systems as its organizing framework to broadly engage Stanford faculty and students, as well as the broader community of experts in industry and government, in improving knowledge and understanding of the fundamental policy issues raised by the integration of cyber technologies.

Promoting engagement, collaboration and partnership was a central goal during the first two years of the Initiative. The Initiative pursued this goal by hosting, sponsoring or otherwise supporting the following activities relevant to cyber policy: (1) the production and dissemination of faculty research that informs and frames policy debates, (2) curricular and extracurricular offerings for Stanford students, (3) education programs for audiences outside Stanford, including business executives, legislative staff, journalists and high-school students, and (4) debates and in-person exchanges of information and views among experts from industry, academia and government. These goals and strategies align with several of those expressed by the Hewlett Foundation’s Cyber Initiative in its Cyber Initiative Refined Grantmaking Strategy 2016, page 5; specifically (referring to the enumeration in the Hewlett document): (1) to build civil society organizations that take a holistic, multidisciplinary approach to cybersecurity and contribute to a more informed policy debate; (2) to educate and expand the knowledge base of existing decision-makers, and educate and empower an emerging generation of cyber policy experts; and (4) to fund new policy relevant research and thought leadership by experts from diverse professional, political, and intellectual perspectives.

As explained later in this Report, the Initiative has achieved considerable success in promoting these goals. It has engaged Stanford scholars across a wide range of disciplines, prompted them to study the ways in which cyber technologies has transformed the systems that they study, encouraged them to build collaborations across disciplines that they had not previously attempted, built partnerships and collaborations with related centers across campus. The Initiative is now recognized as a leading hub at Stanford for the study of the broad range of cyber issues and policy. Details of these accomplishments are provided in the next sections of this Report. As the Initiative begins its third year, it has begun to direct more emphasis on two areas of great policy consequence: (a) the future of the digital economy and (b) the security risks of cyber-reliant systems.
Key Project Developments

This Section summarizes the key project developments over the past year, with description of important research and education activities and work products

1. Research Developments

The primary aim of the Initiative is to promote and support new multidisciplinary and policy-relevant research on cyber issues at Stanford and the principal vehicle for doing so is the yearly university-wide RFP (Request for Proposals) inviting Stanford faculty to submit one or more research proposals. To help identify projects, the Initiative hosted mixers at which Stanford researchers could meet counterparts in other departments to discuss opportunities for joint work. These were very well attended and several collaborations were forged at these events. Fourteen of the Initiative’s supported projects represent newly-formed multidisciplinary collaborations across campus. The Initiative’s executive group makes award decisions after consultation and discussion with the Advisory Committee (see Organizational Structure) and, where helpful, other experts in the relevant fields. Selection criteria, outlined in the RFP and underscored in discussions of the proposals with the Advisory Committee are: focus on a cyber-social system, from the interpersonal to the organizational level; multidisciplinarity of research, often reflected in the collaboration between faculty from different Stanford Schools; novelty and potential impact of the research product; and the balancing of support of exploration of societal and technological questions. Priority in the selection was also given to proposals that promised results that would make contributions to both academic scholarship and to policy, and that would support the development of the cyber-social conceptual framework.

Consistent with these criteria, the awards in 2015-16 and 2016-17 supported broad engagement across Stanford schools and departments, as well as collaboration between technical experts and social scientists. In 2016, a total of $1.1M in research grants was awarded to 11 new research projects (median grant amount: $100K) and $741K in renewals to three research projects from 2015-2016. The research grants for the first two years are summarized in Appendix 1, as are the presentations and publications from each project (further details are available upon request).

As the Initiative moves into its next phase, its executive committee has identified several subject area clusters of research activity that are funded by the Initiative at Stanford and are of profound societal and policy significance. The paragraphs that follow describe some of the projects that lie in two of these subject areas: the future of work and cyber-enabled labor; and the security risks (broadly conceived) of cyber-reliance across various cyber-social systems. The descriptions include the amounts of the grants, the principal investigators, and their presentations and publications.

The future of work: Labor and cyber technologies.

Michael Bernstein, Assistant Professor of Computer Science
Margaret Levi, Professor of Political Science and Director, Center for Advanced Study in the Behavioral Sciences
Ramesh Johari, Associate Professor of Management Science & Engineering
Melissa Valentine, Assistant Professor of Management Science & Engineering
2015-2016: $150,000
2016-2017: $300,000

The nature of work is being reshaped by computational systems, which increasingly draw on massive online labor markets to hire and direct workers’ behavior at scale. Melissa Valentine, Michael Bernstein, Margaret Levi, and Ramesh Johari have developed a crowdsourcing system, Foundry, that can achieve open-ended goals by combining the open call recruitment of crowdsourcing with the more sophisticated and reconfigurable coordination affordances of organizations. The system creates crowd organizations, which automatically hire diverse online experts from massive online labor markets to populate computational structures inspired by organizations (roles, teams, and hierarchies), and then continuously reconfigure these structures to responsively adapt the crowd workers’ activities. This research demonstrates how computational systems can enable digitally networked organizations that flexibly assemble and reassemble themselves from a globally distributed online workforce to accomplish complex work.

In a controlled study, Valentine and her colleagues compared the performance of six teams assigned to take “napkin sketches” or basic concepts for new web applications and design working prototypes. Three teams used the flash-team approach, in which the Foundry system kept all the team members apprised of each other, while three other teams were self-managed. All the teams completed their work, but the flash teams did theirs in half the time. In fact, the slowest flash-team finished its task faster than the fastest self-managed team. Each project required about 30 people with a wide range of skills, and each project leader was able to hire the right people in record time: on average, about 13.7 minutes per person.

Flash teams have profound implications for how organizations work. As more and more tasks are automated or are capable of being completed online and remotely, corporations are restructuring job responsibilities, and many younger workers are working multiple jobs that are mediated by cyber technologies (such as Upwork’s software) and apps. The Foundry platform is proof of concept for nimble, cyber-mediated job completion that drastically improves the processes of hiring and communication that make project completion and personnel management such a lengthy process for government-funded projects, and has policy implications for the Department of Labor (in classifying workers, establishing payment models for projects and for residuals from those projects, and in creating policies for the temporary hiring of foreign skilled workers) and the OPM (in approving personnel to work on government-funded projects remotely, creating teams and hiring workers quickly, and providing remote supervision of government-funded projects).

Presentations:

Publications:


Events

**Cyber risk and security: Crypto Policy Project.**
Dan Boneh, Motwani Professor of Electrical Engineering and Computer Science
Jennifer Granick, Director of Civil Liberties at the Stanford Center for Internet and Society, Stanford Law School
Riana Pfefferkorn, Cryptography Fellow at the Stanford Center for Internet and Society, Stanford Law School
2015-2016: $120,000
2016-2017: $174,000

Encryption helps human rights workers, activists, journalists, financial institutions, innovative businesses, and governments protect the confidentiality, integrity, and economic value of their activities. However, strong encryption may mean that governments cannot make sense of data they would otherwise be able to lawfully access in a criminal or intelligence investigation.

Today, the crypto policy issue has resurfaced. The Crypto Policy Project, led by Jennifer Granick (Stanford Law School) and Dan Boneh (Professor of Computer Science) and assisted by lawyer and cyber fellow Riana Pfefferkorn, investigates and analyzes the policy and practices of the U.S. and foreign governments for forcing decryption and/or influencing crypto-related design of online platforms and services, devices, and products, both via technical means and through the courts. The project’s interdisciplinary approach includes technical analysis of policy proposals for encryption design, and research on the benefits and detriments of strong encryption on free expression, political engagement, economic development, and other public interests.

This project has led to the publication of an amicus brief, numerous blog posts (e.g., Just Security, CIS) and media attention. In October 2015, Granick and Pfefferkorn, together with the American Civil Liberties Union, submitted a proposed amici curiae brief in the Brooklyn case to explain why the All Writs Act did not authorize the government’s unlocking demand. The court chose not to accept the brief, reasoning that Apple’s arguments would suffice to inform the court. Nevertheless, Apple’s subsequent arguments to the court very closely echoed ours. Those arguments prevailed: the court ultimately sided with Apple in a landmark 50-page opinion. That opinion came out at the
end of February 2016. On short notice given the court’s scheduling order, Granick and Pfefferkorn worked with Prof. Boneh to write a brief in support of Apple.

Granick and Pfefferkorn have also initiated efforts to uncover what encryption-related policies and practices the U.S. government has developed outside of the public eye. The team has filed several Freedom of Information Act (FOIA) requests to the Department of Justice (DOJ) for internal or sealed documents about its anti-encryption efforts. In addition to these FOIA requests, Pfefferkorn did a deep dive into federal court dockets to locate and compile any unsealed records of “unlocking” or other encryption-related technical-assistance demands to Apple and Google regarding encrypted smartphones.

Publications
Granick, J., Pfefferkorn, R. Brief of amici curiae iPhone security and applied cryptography experts in support of apple, Inc.’s motion to vacate order compelling Apple, Inc. to assist agents in search, and opposition to government’s motion to compel assistance. March 2016.

Events
Policy, Law, and Technology in the Current Crypto Wars. 11/2/2016. Paul Brest Hall, Stanford. 150 attendees from civil society, academia, and law.

Cyber risk management: Cyber insurance and financial cost of breaches.
Michael Klausner, Nancy Charles Munger Professor of Business and Professor of Law, Stanford Law School
Ben Lawsky, Cyber Initiative Visiting Scholar, former Superintendent of Financial Services for New York State
George Triantis, Charles J. Meyers Professor of Law and Business, Stanford Law School
2016-2017: $100,000

Most of the publicly available data about the cost of breaches to business corporations are the result of surveys and publicly and commercially available cyber-breach data are regarded by many to be inaccurate, incomplete and not organized in such a way as to support analysis. Professors Klausner and Triantis of Stanford Law School are leading a new project, in collaboration with a large cyber-risk insurance broker, to collect cost-data related to breaches of publicly traded firms between 2007 to the present. Their project draws on thorough examination of publicly available sources, including filings with the Securities Exchange Commission, Federal Trade Commission enforcement releases, PACER federal court filings, state breach disclosure websites and national news stories.

When faced with the possibility of a multi-million dollar breach, most companies will attempt to insure themselves against the most common losses experienced by businesses of their industry. But, what does an average cyber insurance policy look like? What coverage areas and terms are standard, and how do these terms stand up in court? The Initiative is funding a study -- led by Visiting Scholar Ben Lawsky and
Professor George Triantis, and in collaboration with members of the insurance industry – of policy coverage, limits and conditions. The project also studies the adequacy of existing coverage of potential catastrophic and interconnected cyber incidents, and considers what the likely political and economic fallout will be from limits in such coverage.

Events
Cyber Insurance: Assessing Risk. May 9, 2016. 100 participants, half from industry. Cyber.stanford.edu/insurance

Dr. Bahman Bahmani, Researcher, Stanford Department of Computer Science
David Mazieres, Professor of Computer Science
Russell Poldrack, Professor of Psychology
2015-2016: $150,000
2016-2017: $170,000

While insurance can provide a partial safeguard against financial losses, a better strategy would minimize the possibility of those losses altogether. Attempts at improving consumer security have focused on passwords, challenge questions, out-of-band text messages, and physiological biometrics that create friction with user experience, and yet are increasingly bypassed by hackers. Our research on behavioral biometrics, led by Professor of Psychology Russell Poldrack and Professor of Computer Science David Mazieres, studies the use of behavioral biometrics, i.e., the unique traits in user interactions with digital devices and services, for frictionless cyber authentication. Due to the critical importance of authentication in online and mobile banking and financial services, our research focuses on and analyzes the effectiveness of behavioral authentication schemes for use cases in this sector. In particular, the Behavioral Biometrics team studies the application of behavioral biometrics in detection of sophisticated cyber threats such as remote access trojans, the ease of use offered by cognitive authentication, and the robustness of behavioral biometrics authentication against adaptive adversaries actively circumventing the system. The results of this project, only one year in, have already led to patent applications, the potential scope of the applied solutions being developed is large.

Publications
Two patent applications are under review

Publications from other research projects funded by the Initiative are listed with their respective project descriptions in Appendix

2. Education Developments

The Initiative’s education efforts encompass education at Stanford (e.g., seminars, courses, and student groups) and programs aimed at audiences beyond Stanford (e.g., conferences, publications, public media, executive education). Given Stanford Cyber Initiative’s broad mission, as described in the grant proposal of 2014 and elaborated on the website (https://stanford.cyber.edu), the Initiative aims, through education, to convey knowledge
relating to policy issues concerning the security of cyber-reliant systems, as well as to promote appreciation for the importance of a multidisciplinary study of the fundamental effects of cyber technology on society (particularly approaches that combine technological and social science expertise). Cyber-social systems are a new concept (or at least a new term) for most people, and the Initiative has sought to popularize the concept and encourage thinking about cybersecurity from societal and human perspectives. The educational initiatives range from high-school curriculum to executive education courses, and are summarized below in the categories of (a) courses directed to Stanford students that are taught by directors of the Stanford Initiative and (b) conferences and events available to audiences outside Stanford that were hosted or supported financially by the Initiative or benefited from the participation of Initiative directors. The Initiative has encouraged faculty and affiliates to offer or undertake the development of multidisciplinary courses related to their research, which usually does not require additional funding. Its executive is evaluating whether this activity merits the creation of a full degree program or track.

Courses taught in 2016-17 by Cyber Initiative directors for Stanford students

- MS&E 297: Solving National Security Issues with the Lean Launchpad. Boneh and Berke advised a student team of four undergraduates working on an anti-phishing project for the NSA. Spring 2016.

Conferences and Events in 2016-17 for broader audiences

- **Cyber Insurance: Assessing Risk.** May 9, 2016. 100 participants, half from industry. Non-Stanford Speakers: Lauri Floresca (SVP & Partner, Woodruff Sawyer); Peter Beshar (Executive VP & General Counsel, Marsh & McLennan); Tyler Gerking (Partner, Farella Braun); Eric Rosenblum (Forward-Deployed Engineer, Palantir); Paul VanderMarck (Chief Strategy Officer, Risk Management Solutions); Claude Wagner (Chief Actuary, Symantec); Scott Stransky (Assistant Vice President and Principal Scientist, AIG Worldwide); Ben Lawsky (Lawsky Group and Stanford; Former Superintendent of Financial Services, New York State); David Jones (California Insurance Commissioner); Tracie Grella (Global Head of Cyber Risk Insurance, AIG). Cyber.stanford.edu/insurance Fully funded by the Cyber Initiative
- **Cyber Day: Conference for Directors and C-Level Executives.** Jointly organized and hosted with the Rock Center for Corporate Governance. Oct 28th, 2016. 50 attendees from industry and law. Non-Stanford Speakers: Suzanne Spaulding (Under Secretary for the National Protection and Programs Directorate (NPPD) at the Department of Homeland Security); Greg Clark (CEO, Symantec); George Kurtz (President, CEO, and Founder, Crowdstrike); Suzanne Vautrinot (President, Kilovolt Consulting, Inc. and Major General and Commander, USAF (retired); Director, Wells Fargo Corporation, Symantec Corporation, Ecolab Inc.); Lauri Floresca (Senior Vice President, Corporate & Executive
Half of Boot Camp costs ($100,000) provided by the Cyber Initiative.

Sean Sposito, San Francisco Chronicle (Cybersecurity Reporter). Held at Stanford.

Correspondent); Sara Sorcher, Post (Right Turn Blogger); Jay Solomon, Wall Street Journal (Foreign Affairs Producer); Howard Rosenberg, CBS (Producer, 60 Minutes); Jennifer Rubin, Washington Post (Contributing Editor); Michael Isikoff, YAHOO News (Chief Investigative Correspondent); Carrie Johnson, NPR (Justice Correspondent); Mary Kissen, Wall Street Journal (Editorial Board Member); Elise Labott, CNN (Global Affairs Correspondent); Eli Lake, Bloomberg View (National Security & International Affairs Columnist); Carla Marinucci, POLITICO (California Playbook Reporter); Damian Paletta, Wall Street Journal (National Security & Intelligence Reporter) Ben Pauker, Foreign Policy (Executive Editor); Nicole Perlroth, New York Times (Technology Reporter); Shimon Prokupecz, CNN (Crime & Justice Unit Producer); Gabe Ramirez, CNN (Senior Producer); Howard Rosenberg, CBS (Producer, 60 Minutes); Jennifer Rubin, Washington Post (Right Turn Blogger); Jay Solomon, Wall Street Journal (Foreign Affairs Correspondent); Sara Sorcher, Christian Science Monitor (Deputy Editor, Passcode); Sean Sposito, San Francisco Chronicle (Cybersecurity Reporter)). Held at Stanford. Half of Boot Camp costs ($100,000) provided by the Cyber Initiative.

Funded by registration fees.

- **Applied Cybersecurity Student Team.** The Stanford team competed in the WRCCDC (Western Regional Collegiate Cyber Defense Competition) and the Atlantic Cyber 9/12 Competition.
  Team travel and registration fees funded by the Cyber Initiative.

- **Monthly seminar series.** Regular events including research panels (e.g., Behavioral Research and Decision-Making, featuring Ashish Goel, Naomi Grewal of SurveyMonkey, Rob MacCoun, and Jeff Hancock; Personalizing Demography with the World Bank and Worldview Stanford), big names and debut events (e.g., CA Attorney General Kamala Harris joined us to debut the 2016 CA Data Breach Report, and filmmaker Werner Herzog joined us and a standing-room-only crowd of 200+ for a Q&A and the West Coast debut of his film *Lo and Behold: Reveries of a Connected World*, and behind-the-scenes discussion of government agencies’ work on cybersecurity (e.g., a DHS session on red-teaming and security assessment, a behind-the-scenes look at FCC policy-making from our Washington fellow, and an examination of how the NSA’s work has changed pre- and post-Snowden from senior executives at the NSA and the ONI). Event costs funded by the Cyber Initiative.

- **Cyber Boot Camp.** May 15-16, 2016. 25 attendees from US media organizations. (Jim Avila, ABC (Senior National Correspondent); Bryan Bender, POLITICO (National Security Editor); Tom Bevan, Real Clear Politics (Co-founder & Executive Editor); Paresh Dave, Los Angeles Times (Reporter); Jackson Diehl, Washington Post (Deputy Editorial Page Editor); Ryan Evans, War on the Rocks (Founder & Editor-in-Chief); Jennifer Griffin, FOX News (National Security Correspondent); Elias Groll, Foreign Policy (Staff Writer); Jim Hoagland, Washington Post (Contributing Editor); Michael Isikoff, YAHOO News (Chief Investigative Correspondent); Carrie Johnson, NPR (Justice Correspondent); Mary Kissen, Wall Street Journal (Editorial Board Member); Elise Labott, CNN (Global Affairs Correspondent); Eli Lake, Bloomberg View (National Security & International Affairs Columnist); Carla Marinucci, POLITICO (California Playbook Reporter); Damian Paletta, Wall Street Journal (National Security & Intelligence Reporter) Ben Pauker, Foreign Policy (Executive Editor); Nicole Perlroth, New York Times (Technology Reporter); Shimon Prokupecz, CNN (Crime & Justice Unit Producer); Gabe Ramirez, CNN (Senior Producer); Howard Rosenberg, CBS (Producer, 60 Minutes); Jennifer Rubin, Washington Post (Right Turn Blogger); Jay Solomon, Wall Street Journal (Foreign Affairs Correspondent); Sara Sorcher, Christian Science Monitor (Deputy Editor, Passcode); Sean Sposito, San Francisco Chronicle (Cybersecurity Reporter)). Held at Stanford. Half of Boot Camp costs ($100,000) provided by the Cyber Initiative.
  Funded through Cyber Initiative grant.

• **Crypto Policy Project: Policy, Law, and Technology in the Current Crypto Wars.**
  11/2/2016. Paul Brest Hall, Stanford. 150 attendees from civil society, academia, and law. Keynote speakers: Paul S. Grewal (Former Magistrate Judge, Northern District of California); Hon. Stephen W. Smith (Magistrate Judge, Southern District of Texas)
  Half of event costs ($6,000) provided by the Cyber Initiative.

• **Academic Records and Evaluation in the Digital Era: Student Data and Records in the Digital Age.** June 15th-17th peer convening at the Asilomar Conference Grounds in Pacific Grove, CA, to develop first principles for the responsible use of student data in higher education and set priorities for a national/global research agenda for higher education improvement. A digital record of that convening may be found at https://sites.stanford.edu/asilomar/
  Event funded through Cyber Initiative grant.

• **Campaign of the Future: Conference on the Digital Campaign.** 25 participants from industry, media, and government. Invite-only. Non-Stanford Speakers: Erika Franklin Fowler (Wesleyan Media Project); Zeynep Tufekci (New York Times); Coco Panel (Google); Katie Harbath (Facebook); Nu Wexler (Twitter); Molly Schweickert (Cambridge Analytica); Aaron Strauss (Analyst Institute); Joe Rospars (Blue State Digital); Jeremy Bird (270 Strategies); Christie George (New Media Ventures); Ginny Hunt (White House Office of the CTO); Anthea Watson Strong (Google); Daniel Souweine (CEL Climate Lab); Josh Tucker (NYU); Emilio Ferrara (USC); Samuel Woolley (Oxford/UW); Daniel Kreiss (UNC); David Karpf (GW).
  12/2/2016
  Event funded through Cyber Initiative grant.

**Collaboration**

As described above, the goal of the Initiative is to encourage research and thinking about cyber-social systems that encompass both the social and technological advances and concerns associated with the integration of cyber technologies into society. The involvement of expertise from social, humanistic, technological, and scientific disciplines leads to comprehensive analysis of the effects of these technologies from multiple perspectives. Cross-disciplinary collaboration has been essential in the production and dissemination of multidisciplinary research results funded by the Initiative, and the Initiative has also collaborated with a number of organizations within and beyond Stanford. The following are examples of activities jointly pursued between the Initiative and other groups at Stanford over the past year:

• **CIS (Center for Internet and Security, Stanford):** Crypto Policy Project and Crypto Policy Project Readout; Conference on the Vulnerability Equities Process.

• **CISAC (Center for International Security and Cooperation):** China Track II Diplomacy project and equal co-sponsorship of the Cyber Boot Camp (Congressional Staffer Cohort
in 2015 and Cybersecurity Media and Journalist Cohort in 2016, with funding continuing in 2017 and 2018)

- Security Lab (Stanford Department of Computer Science): Crypto Policy Project and sponsorship for the Real World Cryptography conference.
- The Rock Center for Corporate Governance (Stanford Law School): collaboration for the presentation of, and participation in, Cyber Day, a yearly executive education program on cybersecurity for boards of directors and C-level executives, as well as the cybersecurity panels in Stanford Law School’s Directors’ College and the Stanford-Rotman Corporate Governance Day in Canada.
- Worldview Stanford: Collaboration to produce the Raw Data podcast (described further in the Communication section), and our media strategy.

Beyond Stanford, several of our research projects involve collaborations:

- Cyber Insurance project: early-stage collaboration with Symantec
- Costs of Cyber Breaches project: collaboration with insurance broker JLT, Inc.
- Conference on Blockchain Protocol and Security Engineering: collaboration with BCG’s Digital Initiative
- Upcoming conference on the Rule of Law and Cybersecurity: collaboration with the Atlantic Council and Dentons law firm
- The Initiative has also engaged the advice and research participation of external stakeholders including Ben Lawsky (The Lawsky Group; formerly New York State Department of Financial Services), Jonathan Mayer (FCC Chief Technologist for Enforcement), Peter Beshar (Executive VP & General Counsel, Marsh & McLennan), Teresa Shea (Executive Vice President, In-Q-Tel), Sean Brooks (Privacy Engineering head, NIST), and Sean McAfee (DHS Silicon Valley head).

In addition, members of the Initiative had met with a number of state, federal, and international policymakers, including the following:

- James Trainor – FBI: Berke spoke with on 1/25
- Oliver Rosenbloom – CA Governor’s Office of Business and Economic Development: Berke met with on 2/16
- Kamala Harris – CA Attorney General: Seminar on 2/16
- Eviatar Matania – Israeli National Cyber Bureau Chief: Seminar on 2/29 and meeting with Boneh
- Judy Chock – FBI: Berke met with on 3/31
- Sean McAfee – DHS: Seminar 4/25; numerous email conversations
- Herzliya conference: Boneh met with numerous Israeli researchers and policy makers during a trip to Israel with the Hewlett Foundation and spoke at this conference 6/14-6/15
- Lynwen Connick - Australia’s First Assistant Secretary of Cyber Policy: Berke met with on 8/26
- Jeffrey Bleich – Australian Ambassador: Berke met with on 8/26
- MK Palmore – FBI: Participated in Cyber Day on 10/28
• Marina Kaljurand – Estonian Foreign Ministry cybersecurity advisor and former Ambassador to the US: Berke met with on 11/8
• Victor Dodig, CEO of the Canadian Imperial Bank of Commerce: Triantis met with and was co-panelist with on 11/18
• Ed You – FBI: Berke met with on 12/16

Communication and Outreach

This Report identifies in previous sections the communication of research, as well as the organizing concept of cyber-social systems, through presentations, conferences and publications. In addition, the directors of the Initiative have been active in speaking at a number of events outside Stanford and with public media outlets. In addition to the events listed in previous sections, the Initiative’s directors have participated in:

• California State Bar-hosted Symposium on “How to Navigate the Complexities Found at the Intersections of Cybersecurity, Corporate Governance and Government Regulations”
• Panel on Security and Privacy as part of the course Behind and Beyond Big Data produced by Worldview Stanford (an innovative Stanford University initiative that creates interdisciplinary learning experiences)
• Stanford-Rotman Corporate Governance Day at the University of Toronto
• Summit D&O Conference, Park City, Utah panel on "Cyber Security Policy for Boards and the Nation"
• CodeX Future Law conference on legal technologies
• Serving as expert sources for media reporting on cyber-related topics (CSO Online, Mic, EconoTimes, Los Angeles Times)

Two of the Initiative’s outreach efforts targeted at broader audiences are the Raw Data podcast and the Cyber Bytes weekly newsletter. Both have audiences that include members of the tech industry, journalists, government staffers, and philanthropists. These programs bolster the Initiative’s mission of being a reliable source for news, analysis, and research findings.

The Raw Data podcast is entering its second season after a 12-episode first-season run that brought in 6,000+ listeners per episode and landed in the iTunes top 100 for its debut episode. The audio format enables the Initiative to share the work of its researchers in their own words, talk to tech and civil society leaders, and explore the societal consequences of cyber technology in healthcare, government, finance, education, and privacy, to name a few topics from Season One. The hosts, Dr. Michael Osborne and Leslie Chang of Worldview Stanford have NPR experience (Chang) and run a second acclaimed podcast, Generation Anthropocene, on the effect of human activity on the environment.

The Initiative’s weekly newsletter, Cyber Bytes, is distributed on Fridays and has not missed a week since its debut. Authored by the Initiative’s Executive Director, Allison Berke, it has a circulation of over 800 subscribers, both internal and external to Stanford, and has had positive week-over-week subscriber growth since its inception. The newsletter aims to bring the Initiative’s perspective on what is important in cybersecurity and cyber technology news, advancing the Stanford Cyber Initiative brand as a source for insightful commentary and curation on interesting cyber topics.
The Initiative co-sponsors (with the Hoover Institution), and provides annually $100,000 or half the funding for, the Cyber Boot Camp. The Boot Camps are a series of educational events aimed at Congressional staffers and journalists and media professionals reporting on cybersecurity policy (May 15-16, 2016; 25 participants from media organizations across the American ideological spectrum. Attendees are listed in the Conferences and Events section of Key Project Developments, above). The goal of the Boot Camps is both to provide the educational fundamentals of cybersecurity and cyber technology to those who will then create intelligent news stories and well-informed policy decisions on these topics. The boot camps have the added benefit of exposing the attendees to the work and expertise of Stanford researchers. The 2016 boot camp encouraged journalists -- from CNN, 60 Minutes, Fox News, Foreign Policy, the Wall Street Journal, and the Christian Science Monitor -- to consult more often with Stanford researchers on cyber-related topics.

Executive Director Allison Berke also organizes and hosts a monthly seminar series at Stanford, funded by the Initiative, to expand discussion and dissemination of research results on cyber-social topics among the Stanford community. The seminar series draws an audience that includes undergraduates, graduate students, faculty, staff, and community members to hear talks that alternate between:

- Research panels, e.g., Behavioral Research and Decision-Making, featuring Professor Ashish Goel, Naomi Grewal of SurveyMonkey, Professor Rob MacCoun, and Professor Jeff Hancock; Personalizing Demography with the World Bank and Worldview Stanford
- Debut events, e.g., the Initiative hosted California’s former Attorney General Kamala Harris’ public presentation of the 2016 CA Data Breach Report, and filmmaker Werner Herzog joined the Initiative and a standing-room-only crowd for a Q&A and the West Coast debut of his film Lo and Behold: Reveries of a Connected World
- Behind-the-scenes discussion of government agencies’ work on cybersecurity, e.g., a Dept. Homeland Security session on red-teaming and security assessment, a behind-the-scenes look at FCC policy-making from the Initiative’s White House Fellow Jonathan Mayer, and an examination of how the NSA’s work has changed pre- and post-Snowden from senior executives at the NSA and the ONI.

These seminars keep external contacts engaged with the Cyber Initiative and are part of an ongoing conversation that the Initiative is framing on how cyber technologies are influencing society.

**Impact**

As described earlier in this Report, the Initiative’s goals in its first two years have been to maximize awareness, engagement, and cross-disciplinary activity in policy-relevant research and debate concerning cybersecurity and the challenges of cyber-social systems. While quantitative measures of success in pursuing these goals are difficult to identify, there is evidence of achievement. Since its inception, the Initiative has witnessed increased interest in, and activity around, the study of the integration of cyber technologies into society. Many more faculty—17 in Cyber Initiative-funded projects alone—are engaged in the study of cyber technologies and cyber-social systems than when the Initiative began to promote the idea, many due to individual conversations with the Initiative’s executive team to encourage researchers to foster
burgeoning interests in the impact of cyber technologies. There are significantly more collaborations across campus and across disciplines – particularly between engineers and social scientists. Fourteen of the Initiative’s 22 total research projects represent wholly new multidisciplinary collaborations, in some cases between faculty who met at one of the Initiative’s mixers.

The Initiative’s impact is also reflected in the audience for its publications, event attendance, as well as the growth of a network of associations in industry and government. As the Initiative builds capacity and interest throughout Stanford, success is reflected in the activity it helps to generate on campus around topics of cybersecurity, cyber policy, and cyber technology; the creation of a student group (Applied Cybersecurity) specifically to educate and provide opportunities for undergraduates in the fields of cybersecurity and cyber policy; the publications and accomplishments of grantees (see Research Outputs in the previous section); and the fact that it is increasingly recognized as a convener and center for rigorous study in the selected areas of focus (e.g., cyber insurance, blockchain technology and crypto currencies, and the future of work).
Appendix 1: Funded Research Project Descriptions

Key: Category, Title (Amount funded, Dates funded; Faculty and Researchers involved (Faculty Affiliations))

Democracy & Politics

Campaign of the Future
Bruce Cain (Charles Louis Ducommun Professor in Humanities and Sciences and Senior Fellow at the Woods Institute for the Environment)
Nate Persily (James B. McClatchy Professor and Professor, by courtesy, of Political Science and of Communication, Stanford Law School)
$80,000, 2015-2016

Technological advances in voting, communication, and fundraising are changing American campaigns and elections in fundamental ways. Developments in microtargeting, web-based campaign advertisements, and even voting, itself, promise to empower new actors in campaigns and reshape the landscape for political communication. American democracy’s move on-line will have profound implications for the future of traditional intermediary institutions, especially political parties, which have served as the primary avenues for individual participation and representation. The project on the Campaign of the Future seeks to bring together the relevant actors in the campaign system to analyze these trends in political communication, mobilization, and voting, and to assess their impact on American democracy. The project will involve conferences of academics and other experts, an edited volume, and a sole-authored book. For results see the Research Outputs section of the main text.

Crowdsourced Democracy
Ashish Goel (Professor of Management Science and Engineering)
Larry Diamond (Senior Fellow at the Hoover Institution and the Freeman Spogli Institute for International Studies and Professor, by courtesy, of Sociology and of Political Science)
$50,000, 2015-2016

YouTube competes with Hollywood as an entertainment channel, and also supplements Hollywood by acting as a distribution mechanism. Twitter has a similar relationship to news media, and Coursera to Universities. But Washington has no such counterpart; there are no online alternatives for making democratic decisions at large scale as a society. As opposed to building consensus and compromise, public discussion boards often devolve into flame wars when dealing with contentious socio-political issues. This project aims to (a) Design systems that are geared towards structured discussion and consensus decisions, as opposed to towards a free-flowing conversation that degenerates into vitriol, (b) Develop an algorithmic and game-theoretic understanding of voting, decision, and incentive mechanisms, and (c) Deploy these systems in real-life crowdsourced democracy processes, and evaluate them rigorously.

Publications
Goel, A. Decision-making at Scale: A Practical Perspective. Keynote, HCOMP 2016,
It is well known that the cyber relationship between China and the United States is a source of great friction between the two nations. As a step towards improving the cyber relationship, the CISAC/Hoover cyber program will seek to build a sustainable and ongoing dialogue with China, through an initial effort to conduct cooperative research on cybersecurity-related issues. This cooperative effort involves two workshops, one held at a Chinese university and another at Stanford. These workshops (and the resulting publications) should be regarded as a proof of concept that a productive dialogue between Stanford and the Chinese is possible, and funding from a variety of sources would be sought after this project to expand the dialogue and to make it more sustainable.

Law & Law Enforcement

John Duchi (Assistant Professor of Statistics and of Electrical Engineering and, by courtesy, of Computer Science)
Jennifer Pan (Assistant Professor of Communication and, by courtesy, of Political Science and of Sociology)
$50,000, 2016-2017

We aim to develop a methodology to generate the first rigorous scientific measure of a variable of paramount importance to academics and public policy makers worldwide -- the prevalence, location, and scale of collective action events and repression of these events in authoritarian regimes. There is on-going debate over whether cyber technologies threaten the survival of authoritarian regimes by facilitating collective action or whether authoritarian regimes are using cyber technologies to strengthen their rule. We propose to develop an independent measure of collective action and the regime’s repressive response to social mobilization by developing algorithms to detect these activities by using unstructured digital data, including images and text, generated by individuals who witness these events and publicly shared on social media platforms.

Publications

Crypto Policy Project
Dan Boneh (Rajeev Motwani Professor of Computer Science in the School of Engineering and Professor of Electrical Engineering)
Jennifer Granick (Director of Civil Liberties, Center for Internet and Society, Stanford Law School)
$120,000, 2015-2016
$174,000, 2016-2017

Encryption helps human rights workers, activists, journalists, financial institutions, innovative businesses, and governments protect the confidentiality, integrity, and economic value of their activities. However, strong encryption may mean that governments cannot make sense of data they would otherwise be able to lawfully access in a criminal or intelligence investigation. In the 1970s, and again in the 1990s, U.S. government struggled with tradeoffs between its surveillance/law enforcement missions (potentially thwarted by crypto) and its information assurance/crime prevention missions (furthered by crypto). In the main, these debates were resolved in favor of allowing the proliferation of strong crypto. Today, the crypto policy issue has resurfaced. FBI Director James Comey chides Apple and Google for using cryptography architectures that the companies are unable to decrypt for law enforcement. In secret, the intelligence community is invested in breaking popular encryption schemes, stealing encryption keys, and finding ways to circumvent communications security protocols. The Crypto Policy Project investigates and analyzes the policy and practices of the U.S. and foreign governments for forcing decryption and/or influencing crypto-related design of online platforms and services, devices, and products, both via technical means and through the courts. The project’s interdisciplinary approach includes technical analysis of policy proposals for encryption design, contributed by cryptography researchers in the Stanford Computer Science Department’s Applied Cryptography Group. The project also researches the benefits and detriments of strong encryption on free expression, political engagement, economic development, and other public interests. More information about the Crypto Policy Project can be found at https://cyberlaw.stanford.edu/our-work/projects/crypto-policy-project.

Finance

Behavioral Biometrics
David Mazieres (Professor of Computer Science)
Russell Poldrack (Albert Ray Lang Professor of Psychology)
Bahman Bahmani (Research Engineer, Department of Computer Science)
$150,000, 2015-2016
$170,000, 2016-2017

Authentication is one of the major problems faced by the society in interacting with cyber technology. Passwords, challenge questions, out-of-band text messages, and physiological biometrics create friction with user experience, and yet are increasingly bypassed by hackers. In this project, we will study the use of behavioral biometrics, i.e., the unique traits in user interactions with digital devices and services, for frictionless cyber authentication. We will use a principled approach based on human cognitive psychology, systems security, and data mining to design authentication schemes based on behavioral biometrics. Due to the critical importance of authentication in online and
mobile banking and financial services, we will focus on and analyze the effectiveness of our authentication schemes for the use cases in this sector. Further, taking a cyber-social perspective, we will study societal aspects such as data protection legislation and policy, financial regulation compliance, and usability, as well as operational aspects such as personnel and economic impacts, deployment models, and maintenance requirements.

**Costs of Cyber Data Breaches in Public Companies**
*Michael Klausner (Nancy and Charles Munger Professor of Business at Stanford Law School)*
*George Triantis (Charles J. Meyers Professor of Law and Business, Stanford Law School)*
*$100,000, 2016-2017*

This project addresses the need for quantitative measures of the costs incurred by publicly traded companies that experience cyber data breaches. The currently available information is focused more on frequency than severity of breach, including the scope and costs of breach. Most of the publicly available data is the result of surveys and the commercially available cyber-breath data are regarded by many to be inaccurate, incomplete and not organized in such a way as to support analysis. This project collects a broad set of data relating to the costs that publicly traded firms have incurred as a result of breaches from 2007 to the present. For its sources, it draws on thorough examination of publicly available sources, including filings with the Securities Exchange Commission, Federal Trade Commission enforcement releases, PACER federal court filings, state breach disclosure websites and national news stories.

**Health & Medicine**

**Advancing AI Research to Help Policymakers Affordably Improve Life’s Starts and Finishes**
*Fei-Fei Li (Associate Professor of Computer Science)*
*Arnold Milstein (Professor of Medicine)*
*$100,000, 2016-2017*

Understanding grows about childhood experiences occurring primarily in lower and middle class homes that limit fulfillment of children’s’ developmental potential. Simultaneously nations and US state governors face rising demand for costly institutional care that many seniors’ dread. In the United States, the cost of long-term care would more than double from 1.3% of US GDP in 2010 to 3% of US GDP in 2050 if the rate of functional limitations among those age 65 and older remains constant (Congressional Budget Office, 2013). These two trends confront policy-makers with painful fiscal trade-offs. The prior watershed decade was the first in which Medicaid funding demands fueled by institutional spending for seniors’ care exceeded state funds available to fund children’s’ education. Rapid advances in the capability and affordability of in-home AI systems may enable policymakers to more affordably and effectively serve these two vulnerable populations during life’s starts and finishes. Effective, scalable uses of prior generations of cyber systems have improved value-for-money in other service sectors such as airlines and banking. However, use of modern AI capabilities to improve the value of more intimate interpersonal human services is fraught with hope and fear for seniors, families, health professionals, educators and policymakers seeking to serve them cost-effectively. Both emotions are well-founded.
Stanford faculty, fellows, and students from its schools of engineering and medicine seek to formulate and test psychologically nuanced applications of AI in order to increase policy-makers' and industry's understanding of how modern AI systems can more affordably and effectively enable care planners to select in-home care plans that will generate the largest gains in seniors' self-care capabilities.

Resilient and Robust Connectivity for Medical Devices in the Developing World  
Leonore Herzenberg (Department of Genetics Professor)  
Keith Weinstein (Assistant Professor of Computer Science and, by courtesy, of Law)  
$100,000, 2016-2017

The practice of medicine increasingly relies on large quantities of data—often, gigabytes from imaging, genomics, or blood-based analysis. But the medical devices that collect this data are generally designed with the assumption that Internet access is robust and always on. In the developing world, this assumption breaks down. From Addis Ababa to Zomba, cellular networks are typically the best available connectivity, and these networks experience chronic brownouts and fluctuations. The result: blood-pressure monitors, flow cytometers, and MRI scanners all function poorly, unable to send data where it can be analyzed. We have developed a relationship with medical clinics operated by the U.S.-based Clinton Health Access Initiative (CHAI) in Kenya, Ethiopia, Zimbabwe, Malawi, and Uganda. We propose to kick-start a project to design and deploy a series of reliable Internet gateways boxes at these sites. We will use two main approaches: (1) a “robust tunnel” that masks brownouts with computer-networking techniques (e.g. aggressive retransmission and error-correction coding) to construct more-reliable connectivity out of multiple less-reliable cellular links, and (2) a “self-incentivizing network” that rewards anybody who successfully carries uploads from the medical facility to the Internet, by publicly offering to pay money in exchange for carrying an encrypted dataset to the cloud.

Cybersecurity of Health Care Data in Population-Based Health Information Exchanges  
Dan Boneh (Rajeev Motwani Professor of Computer Science in the School of Engineering and Professor of Electrical Engineering)  
Mark Cullen (Professor of Medicine)  
Lorene Nelson (Associate Professor & Chief, Division of Epidemiology in the School of Medicine)  
Michelle Mello (Professor of Law and of Health Research and Policy, Stanford Law School)  
Nigam Shah (Associate Professor of Medicine (Biomedical Informatics Research) and of Biomedical Data Science)  
$100,000, 2016-2017

Health information exchanges (HIEs) integrate electronic health records from multiple healthcare facilities in a geographic region, and secondary use by researchers of the data from these large generalizable samples have tremendous potential for benefitting population health and informing public policy. Although state and federal laws provide some architecture for protecting healthcare information privacy, most of these laws predate and do not contemplate the recent explosion in the number of online information sources, leaps in computing capabilities, and rise in hacking incidents. The absence of standard data sharing guidelines with rigorous privacy guarantees has made health care organizations afraid to share data, posing significant hurdles for the
population health research use of HIE data. An interdisciplinary group of faculty with expertise in population health, epidemiology, computer science, statistics, health policy, bioethics and law will address these challenges from two perspectives: (1) societal, legal and health policy aspects, assessing the public’s views regarding HIE privacy risks and proposing legal and policy measures that would better achieve the balance of risks and benefits the public desires; and (2) cybersecurity aspects, addressing the key technological challenges for designing secure encryption systems and statistical techniques and identifying critical gaps where novel solutions are needed.

Cyber Systems in Healthcare Organizations
Mohsen Bayati (Associate Professor of Operations, Information and Technology at the Graduate School of Business and, by courtesy, of Electrical Engineering)
Melissa Valentine (Assistant Professor of Management Science & Engineering)
$150,000, 2015-2016
$98,000, 2016-2017

Advanced cyber-systems hold tremendous promise for transforming modern hospitals, potentially improving their capacity, safety, and operational efficiency by extending limited human ability for memory, judgement, and situational awareness. Yet technologies are not exogenous “interventions” into organizational systems. Instead, they are shaped by and then in turn shape the social system, as people interpret and enact the technologies based on their professional identities or the power dynamics activated by the technology implementation process. Also, at present these systems are technically limited in their ability to support situational awareness and data-driven decision-making. This research project aims to advance understanding of cyber-technology enactment and to advance the frontier of dynamic learning and decision-making in health care organizations. We plan to use ethnographic field research methods and operations research analytics to study and improve two health-care cyber-systems: real-time locating services (RTLS) at the Stanford South Bay Cancer Center and a new Hospital Operations Center (HOC) at the Stanford Hospital.

Cyber Tech in Patient-Physician Relationships
Abraham Verghese (Linda R. Meier and Joan F. Lane Provostial Professor of Medicine)
Jeff Chi (Resident in the School of Medicine), Sonoo Thadaney)
$80,000, 2015-2016

We believe the 20th century was one of technology development, and the 21st century is focused on appropriate and relevant application of technology. The technology in cyber-social health systems promised increased efficiency, improved effectiveness, fewer errors, and global connectivity. However, we’re now aware of the unintended consequences. In modern medicine, particularly in the hospital, the bed-ridden patient has become an icon for computerized patient data - an entity we’ve termed the “iPatient”. The iPatient receives the undivided attention of the medical team, is the subject of discussions on cyber-social medical systems about their medical images and more. The integration of human patients and doctors with medical cyber technologies, such as the electronic patient record and networked tools recording medical data, form a cyber-social medical system. In this system, often the human patient experiences abandonment and wonders - where are the doctors? What is going on? What is the
plan? Who is in charge? The disjunction between the patient’s experiences of inattentiveness is at odds with the physicians’ perception of being very attentive (to the patient’s data), and of providing good medical care. We believe this disconnect stems from the idea that knowledge and data don’t translate to wisdom, a key component in medicine.

Publications

Consumer Markets

Self-Incentivizing Networks
Ramesh Johari (Associate Professor of Management Science and Engineering and, by courtesy, of Computer Science and of Electrical Engineering)
Keith Winstein (Assistant Professor of Computer Science and, by courtesy, of Law)
$30,000, 2015-2016

We are developing the engineering and economic tools to enable self-incentivizing enclaves on the Internet, where entrepreneurs can add incrementally to the network's capacity and be rewarded for their contribution, however small, to encourage the buildout of connectivity in under-served areas. This problem cuts across the domains of congestion-control, traffic engineering, and wide-area routing and settlement on the Internet.

How Intermediaries Affect User Choice in News and Commerce
Susan Athey (Economics of Technology Professor, Senior Fellow at SIEPR and Professor, by courtesy, of Economics)
David Blei
$100,000, 2016-2017

Access to digital information involves intermediaries. For online news, these are web pages and apps provided by news organizations, search engines, news aggregators, portals, and social media. For shopping, intermediaries are primarily e-commerce websites and apps. In such settings, users choose from a large set of alternatives, but the effective alternatives at a point in time are limited by the options presented on a web page or mobile screen. This project develops new methods for estimating user preferences as well as product characteristics from data about user choices, taking into account what options were presented (e.g. the links on the web page they visit). We build on recently developed computational methods for large - scale Bayesian models, adapting the methods to incorporate the specific features of web browsing. We further incorporate insights from economics about how to ensure that estimates reflect fundamental preferences on the part of the users (causality versus correlation). We use the estimates to make counterfactual predictions about questions such as, what would happen if intermediaries changed the way they select news. This helps uncover the forces that shape news consumption today as well as incentives faced by news organizations in the future. We also consider applications to e-commerce.
The interdependence and fragmentation of life experiences across cyber-social systems
Laura Carstensen (Fairleigh S. Dickinson Jr. Professor in Public Policy and Professor of Psychology)
Byron Reeves (Paul C. Edwards Professor of Communication, Senior Fellow at the Precourt Institute for Energy and Professor, by courtesy, of Education)
Nilam Ram
$250,000, 2016-2017

Smartphones and laptop computers now allow multitasking among a greater range of experiences than has ever been possible. People switch between radically different content – from work to play to social relationships – and often within seconds. This means that understanding interchanges with cyber-social systems (e.g., health, social relationships, finances, shopping, transportation, work productivity, learning) will depend as much on stitching together experiences across domains as on examining experiences scattered within any single system. Health interactions influence social relationships, which influence financial decisions, which influence work productivity, and so on. Our project is about the interdependence of cyber-social systems across time domains (i.e., from seconds to years) and spatial locations. Many behaviors now emerge through digital experiences, producing data that can be accessed through portals and accumulated into a cohesive picture of individual life. In Phase 1 we will design, borrow and build software tools that gather, store, search and visualize experiences over time, paying attention to embedded security and privacy issues. In Phase 2 we will use those tools to test hypotheses and explore the interdependences among domains. We will emphasize the communication of data back to individuals and organizations so that each might use insights from cross-domain tracking to improve policies and practices in learning, commerce and social relationships.

Consumer Privacy
Kostas Bimpikis (Associate Professor of Operations, Information and Technology at the Graduate School of Business)
Yonatan Gur (Assistant Professor of Operations, Information and Technology at the Graduate School of Business)
$50,000, 2015-2016

Recent advances in information technology have allowed firms to gather detailed data about consumers’ preferences and the structure of their social interactions. Along with the growingly adopted targeting technologies, the wealth of available information benefits firms and holds a lot of promise for individuals. On the other hand, challenges arise with regards to the sensitive nature of the information entities such as firms and government agencies may collect about individuals. In such a context data holders may take advantage of the individuals’ inability to fully comprehend and anticipate the potential uses of their private information with detrimental effects for aggregate social welfare. These challenges are only amplified by the fact that consumer information is a valuable business asset and it is typically infeasible for an individual to retain full control of its informational value. Moreover, individuals interact with one another forming social relationships and preserving one’s privacy in the context of a connected society which presents another set of interesting questions especially when individuals have
different views on what may constitute sensitive information. This proposal aims to
develop a comprehensive way to think about extracting the significant societal and
commercial value of data about individuals while taking their privacy considerations into
account.

Publications
https://www.gsb.stanford.edu/faculty-research/publications/competitive-targeted-
advertising-over-networks

Secrecy of Sequential Decision-Making
Kuang Xu (Assistant Professor of Operations, Information and Technology at the Graduate
School of Business and, by courtesy, of Electrical Engineering)
$50,000, 2016-2017

The increasing prevalence of large-scale surveillance and data collection infrastructures
deployed by government agencies and private companies has brought global attention
to the astonishing power enabled by modern cyber technologies. While such
information appears to be revealing (e.g., a consumer's past browsing behavior may be
indicative of the final purchase decision), we still lack a satisfactory understanding of the
true value of the data collected, in terms of the extent to which it allows one to predict
an individual's intention or future behavior using his or her past actions. This project
aims to create a new mathematical framework to quantify the fundamental degree of
information leakage associated with an individual’s sequential decision-making process,
as well as design intelligent algorithms and decision-making policies that are capable of
obfuscating an individual's future actions, even against a powerful data collector.

Publications
Xu, Kuang. Forthcoming. "Delay-Predictability Tradeoffs in Reaching a Secret Goal."

Labor

Collective Action and Governance in an Online Piecework Economy
Michael Bernstein (Assistant Professor of Computer Science)
Margaret Levi (Professor of Political Science and Director of the Center for Advanced Study in the
Behavioral Sciences)
$50,000, 2016-2017

The digital gig economy has led to a resurgence of piecework. Without shared factories
and water coolers, how do digital pieceworkers coordinate, build solidarity, and take
collective action? We will engage in fieldwork with digital pieceworkers who work in
data entry, domestic services, and on-demand driving to understand how they counter
algorithmic systems and engage in collective behavior. We will then design and launch a
new collectively-governed platform for gig workers. Our goal is to both understand the factors that drive collective behavior in distributed gig platforms, and to introduce new designs and infrastructure that enable the growth of worker collective action in the digital piecework (gig) economy. Our results shed light on the strengths and weaknesses of digital piecework cooperativism, as well as the policies necessary for it to succeed.

*Cyber Work: The Future of Networked Labor*

*Michael Bernstein (Assistant Professor of Computer Science)*
*Ramesh Johari (Associate Professor of Management Science & Engineering)*
*Margaret Levi (Professor of Political Science and Director of the Center for Advanced Study in the Behavioral Sciences)*
*Melissa Valentine (Assistant Professor of Management Science & Engineering)*

$150,000, 2015-2016
$300,000, 2016-2017

Technology has transformed from a tool that supports work into a comprehensive infrastructure that connects workers to employers. Platforms such as Uber and Amazon Mechanical Turk, which announce themselves as the “gig economy” and “paid crowdsourcing”, signal a shift where workers and employers connect ad-hoc, at large scale, to accomplish complex tasks. This shift to online networked labor has the potential to dramatically reconfigure how we shape our careers, organizations, and market platforms, and in turn shifts how those careers, organizations and platforms shape our society. Inspired by this transformation and its risks, our project addresses challenges facing the entire span of the networked labor ecosystem: individuals, organizations, and the work platform itself. We study three fundamental questions: first, how will people manage their work lives online? Second, how might organizations look in a future of networked labor? Third, how do networked labor platforms succeed? To address these challenges, we propose a combination of social scientific, design and engineering endeavors. Our efforts aim to envision the future of digital work, and to inform and create the technological platforms that enable it.

*Folk Theories of Cyber-Social Systems and their Implications for Privacy*

*Michael Bernstein (Assistant Professor of Computer Science)*
*Jeff Hancock (Professor of Communication)*

$100,000, 2016-2017

As people interact with complex cyber-social systems such as Facebook’s ranked news feed and Uber’s hiring algorithms, they build up folk theories of how these systems work. These theories, however, can often be wrong. For example, many people believed the Facebook news feed to be an unfiltered window of their friends’ behavior, leading to widespread surprise and news coverage when a Facebook experiment on emotional contagion highlighted that Facebook manipulates the content of users’ feeds. We propose to investigate the folk theories that people hold about complex cyber-social systems, and determine whether users’ privacy behaviors on these systems are direct reflections of their folk theories. We then propose targeted design interventions to nudge users’ folk theories. This research highlights how systems and algorithms impact society not only through their direct outputs, but also through the (potentially problematic) understandings that people form of them.
Digital learning environments and data analytics have dramatically expanded what might count as academic records, raising questions about the viability of inherited record systems predicated on paper or paper-equivalent documents and institutionally based verification systems. Engineers and student services professionals at Stanford and worldwide are actively developing academic record systems more appropriate for a digital era. Because academic credentials are increasingly fateful for people’s life chances, all of those who produce and purvey them must do so with careful attention to the privacy and discretion of learners and to the integrity of the human relationships inherent in any instructional process. Our project specifies first principles for the ethical governance of these new technologies.

For results see Research Outputs section in the main text, and ru.stanford.edu

Publications


[http://ru.stanford.edu](http://ru.stanford.edu): An ongoing web presence publicly released in September 2016, titled “Responsible Use of Student Data in Higher Education.” The purpose of this site is to catalyze national/global discussion about how data-driven improvement in higher education can be pursued with high, consistent, and transparent ethical standards.

---

*Cyber-Text Technologies: Presenting the Future of the Past*

*Ronald Egan (Professor of East Asian Languages and Cultures)*

*Elaine Treharne (Professor of English)*

*$100,000, 2016-2017*$
Cyber Text Technologies will ascertain from a small but detailed set of case studies to what extent all forms of human communication might be not only systematic, but also effectively skeumorphic, unconsciously emulative, and to an extent formulaically replicative. We aim to investigate through machine learning that employs refined and targeted modeling whether or not specific conventions and identifiable trends characterize every text technology from Cuneiform to Snapchat. Since text technological transformation is constant and cyclical, it is a definitive goal of this project to attempt to project into the future the ways in which these trends will manifest themselves in the development of new information systems and forms of communication from Virtual Reality to Incorporeal Technologies.
Appendix 2: Cyber Initiative Seminars and Events

(Those not listed in the Outreach section above)

Personalizing Demography Seminar
Jan 29, 2016
Speaker: Dr. Wolfgang Fengler, World Bank
Info: Hosted by Worldview Stanford, CESTA, and the Stanford Cyber Initiative: Big data is transforming what we know about the world and the decisions we make as organizations and individuals. Wolfgang Fengler, Lead Economist for Trade and Competitiveness at the World Bank in Vienna, is pioneering new applications at the intersection of global demographics, visualization, personalization, and policy. In addition to his role at the World Bank, Dr. Fengler is the co-host of the Future Development blog and the cofounder of population.io, which aims to make demography – the study of human populations – accessible to a wider audience. Soon to be at the core of a Silicon Valley start-up in the personalized healthcare space, population.io will answer such questions as: What is my place in the world; how long will I live; and how can I live longer? Join us to hear Dr. Fengler discuss his work on demographics, development, and big data.

Applied Cybersecurity student group: Tim Junio, Qadium CEO; and Cyber Policy Social
Feb 4, 2016
Info: Our affiliated student group Applied Cybersecurity held two events: first, from 4:30-6pm, Tim Junio, CEO of Qadium, have a talk on massive data-gathering and indexing the non-web internet. Then, at 6pm, the group held a policy social for participants to learn more about becoming involved with cybersecurity policy initiatives.

Behavioral Research and Decision-Making in the Age of the Internet
Feb 8, 2016
Speakers: Ashish Goel (MS&E), Naomi Grewal (SurveyMonkey), Jeff Hancock (Communication), and Rob MacCoun (Law)
Info: How are online platforms affecting the collection and analysis of data? How does the internet change the types of research individuals and organizations can conduct? This seminar touched on new models of IRB approval, the reproducibility problem inherent to the use of proprietary data, and the use of platforms like Amazon Mechanical Turk, Survey Monkey, and Facebook to conduct research. The speakers also examined ethical issues with the use of algorithms to automate formerly human-centric decision-making processes involving large amounts of data.

California Attorney General's Office Response to Data Breaches
Feb 16, 2016, 2-3pm
Speakers: Attorney General Kamala Harris and Staff
Info: CA Attorney General Harris and staff unveiled and discussed the 2015 CA Data Breach Report and the AG office’s techniques for addressing cyber crimes including identity theft and hacking. The Attorney General's office established the eCrime Unit in 2011, as part of a focus on cyber safety and cyber exploitation. The eCrime Unit is tasked with investigating and prosecuting large scale identity theft and technology crimes with actual losses in excess of $50,000. The Attorney General's office also tracks data security breaches, which are searchable on their website at https://oag.ca.gov/ecrime/databreach/list.
Symposium: How to Navigate the Complexities Found at the Intersections of Cybersecurity, Corporate Governance and Government Regulations
Mar 8, 2016
Speakers: Paul Luehr (Stroz Friedberg), Sabrina Ross (Uber), Jacob Russell (SLS), Thomas Dahdouh (FTC), Allison Berke (Cyber Initiative), Joanne McNabb (CA DOJ)

Locksport: An Introduction to Ethical Lock-picking
April 13, 2016
Speaker: Applied Cybersecurity student group
Info: This technical session focused on non-destructive methods for defeating locks with simple tools you can make yourself. Topics included basic lock design and a sample of picking, raking, and bypass techniques. Additional time was devoted to discussing the overlap between physical and cyber security.

Lo and Behold: Reveries of a Connected World
April 8, 2016
Speaker: Werner Herzog
Info: The Cyber Initiative co-sponsored a screening and West Coast premiere of Werner Herzog's newest documentary, “Lo and Behold: Reveries of a Connected World”, which is about the effects of the Internet on society. Werner was in attendance, and there was a Q&A after the screening.

Seminar: Red-Teaming and the DHS Approach to Evaluating Cybersecurity
April 25, 2016
Speaker: Sean McAfee (DHS)
Info: Sean McAfee is a Project Lead for the U.S. Department of Homeland Security (DHS), National Cybersecurity Assessments and Technical Services (NCATS) team. He provides subject matter expertise in social engineering and insider threats. Mr. McAfee has worked in various capacities at the Department since 2008. Prior to DHS, he worked as a Grants Administration specialist at the US Department for Health and Human Services. Mr. McAfee holds a Master’s degree in Forensic Psychology from Marymount University. This seminar explored how DHS performs cybersecurity assessments and threat intelligence integration to provide decision-making and risk management guidance to state and local agencies and infrastructure.

Cyber Insurance Conference
May 9, 2016
Speakers: Lauri Floresca (Woodruff Sawyer); Peter Beshar (Marsh & McLennan); Auston Davis (Stanford Children's Health); Tyler Gerking (Farella Braun) Eric Rosenblum (Palantir); Paul VanderMarck (Risk Management Solutions); Dan Boneh (Stanford); Ben Lawsky (Lawsky Group and Stanford); David Jones (California Insurance Commissioner); Tracie Grella (AIG)
Info: The Stanford Cyber Initiative hosted talks and panels on the growing field of cyber insurance. Brokers, underwriters, clients and lawyers analyzed cyber insurance policies and claims, as well as examples of litigation over policies that have shaped coverage conditions. Panelists from government, tech, insurers, and academia proposed and discussed the aspects of cyber risk that should be given the most scrutiny by issuers and customers of cyber insurance. Finally, ideas for policy solutions to beneficially shape the growth of the cyber insurance industry, in the US and as it grows abroad, were proposed and discussed. The discussion...
examined analogous government roles in similar insurance contexts, such as earthquakes, flooding, and terrorism.

**Web Hacking Workshop**  
May 11, 2016  
This technical workshop described how hackers steal password databases and take over websites. This technical workshop provided hands-on experience with web hacking, including attacking a website using cross-site scripting and SQL injection and exploiting the famous Heartbleed and Shellshock bugs to take control of the webserver.

**Web Attacks in the Real World**  
May 18, 2016  
Speaker: Shape Security  
A panel of four recent Stanford graduates working at Shape Security shared their real world "war stories" of combating cyber criminals in the field. The session offered a demo-driven introduction to attacks on real web services and applications, and a glimpse into how the cyber crime and security industry drive each other to create a vibrant economy of attack tools and defense suites.

**Seminar: Lessons from the FCC**  
October 20, 2016  
Speaker: Jonathan Mayer (FCC)  
Info: Jonathan Mayer, chief technologist for enforcement at the FCC, gave a seminar on his work on increasing privacy for internet users. Jonathan's work prior to the FCC includes analysis of telephone metadata, web tracking, and the Computer Fraud and Abuse Act. Jonathan Mayer is a Ph.D. candidate in computer science at Stanford, and a lawyer, having received his J.D. from Stanford Law School in 2013. This seminar is open to Stanford community members only. More information on Jonathan's work is available at https://jonathanmayer.org.

**Seminar: An Inside Look at the NSA**  
October 21, 2016  
Speakers: John Keefe (NSA), Sabra Horne (ONI)  
Info: John Keefe, an NSA executive, Senior Strategist for Computer Network Operations of the NSA and Stanford alumnus, joined us to discuss his work. Mr. Keefe was joined by Sabra Horne, Senior Adviser, Open Source Outreach, Office of National Intelligence. Mr. Keefe's seminar was limited to students.