



KOGOD
CYBERSECURITY
GOVERNANCE
CENTER

PANDEMIC YEARS

2020-2022 • Biennial Report

Business Focused • Data Driven
Human Centric • Risk Aware

LETTER FROM DIRECTOR



When I wrote the letter from director for the last Kogod Cybersecurity Governance Center (KCGC) Report, in June 2020, I thought the time of teaching online and attending virtual events would soon be over, and everything would go back to normal in a matter of months. It didn't cross my mind that we would have a global pandemic that lasts for at least two years, and most of the events I attend today are still either virtual or hybrid.

The global pandemic raised enormous challenges for every aspect of the society.

It also brought sudden yet paradigm-altering changes to the future of our work and life. On issues closely related to KCGC, the pandemic made cybersecurity an even more important issue for corporate governance, as organizations had to shift considerable portions of their activities online, and cyber criminal seized the opportunity to launch treacherous attacks. Education-wise, the pandemic changed the modality of teaching at Kogod for over a year. Yet it also encouraged virtual collaboration among students and forever expanded the ways in which students and teachers could interact both online and offline.

The paradigm-altering changes happening in the society is also indicative of what KCGC researchers have been working on during the pandemic years which, despite the challenges, turned out to be a highly productive and rewarding period of time. During these two years, we gratefully received a new, \$1 million, research grant, jointly sponsored by the National Science Foundation and Amazon.com, Inc., to expand our research into the fairness of Artificial Intelligence (AI), in particular the use of machine

learning algorithms in the context of hiring and promotions. We also received a \$100,000 research gift from Meta Platforms, Inc., to continue our research into people's perceptions, beliefs, and attitudes towards privacy. Meanwhile, we continued our multiple ongoing projects funded by the National Science Foundation (NSF), studying topics from trustworthy analytics over social media to privacy protection over mobile devices and online platforms.

We also disseminated our research results on highly impactful venues. Our journal publications appeared on premier and highly selective venues such as Management Science and Management Information Systems Quarterly (MISQ), both ranked as top business journals by the Financial Times. We presented our research to academic researchers, government agencies, our industry partners and trade associations. KCGC was also represented in panel discussions on many international events, from Europe to Latin America. Even though the pandemic did not allow us to bring speakers to campus, we hosted an incredible line-up of distinguished

Business Focused.
Data Driven.
Human Centric.
Risk Aware.

speakers online at our virtual seminars.

I am proud to see the many achievements of KCGC researchers over the past two years, and I know none of these is possible without your continued support, both in terms of your generous financial sponsorship and the time and advice you so kindly gave us. We sincerely thank you for the meaning you brought to our work, and we look forward to continuing collaborations and partnerships with you in the future!

Heng Xu



AWARDS

IN 2020–2022, KCGC RESEARCHERS
RECEIVED SEVERAL DISTINGUISHED
AWARDS AND RECOGNITIONS

The Inaugural MISQ Impact Award (2021)

From Management Information Systems Quarterly (MISQ), the premier journal for information systems research.



Dr. Heng Xu and her coauthors received the inaugural Management Information Systems Quarterly (MISQ) Impact Award 2021. The award is given to one article published a decade earlier that has had "the most significant and sustained scholarly impact, as shown by citations, by how it led to a change in thinking in the field, and by its prescience in identifying an important issue today" and "a real or potential impact beyond academia, especially through how it influences the way our field engages in an important real-world domain."

LEARN MORE AT
[AMERICAN.EDU/KOGOD/
RESEARCH/CYBERGOV/](https://AMERICAN.EDU/KOGOD/RESEARCH/CYBERGOV/)



2022 Outstanding Scholarship, Research, Creative Activity, and Other Professional Contributions Award

From American University

Dr. Heng Xu received the Outstanding Scholarship, Research, Creative Activity, and Other Professional Contributions Award from American University. The award is given annually to one faculty member who “has achieved distinction as a scholar as documented through publications; invited lectures and papers; performances or shows; leadership in professional societies; work on editorial boards; procurement of major grants; membership in prestigious professional organizations; references, quotes, or appearances in the media; or selective positions of leadership”.



2020 CACM Research Highlight Award

From the Association for Computing Machinery (ACM)

A paper co-authored by Dr. Nan Zhang was selected by the Communications of the ACM as one of the “outstanding research articles selected from the broad spectrum of computing research”.

RESEARCH GRANTS

KCGC RECEIVED RESEARCH GRANTS
FROM NSF, AMAZON, AND META

Fairness in AI: Using Machine Learning to Address Structural Bias in Personnel Selection

Jointly sponsored by the National Science Foundation and Amazon

Today, personnel selection practitioners in the United States are primarily guided by two streams of knowledge: 1) the development on the legal front pertaining to employment opportunities, and 2) the accumulation of findings in social, behavioral, and economic sciences that guide the accepted professional practices in personnel selection. This research project focuses on establishing machine learning as the third pillar for the design of personnel selection systems in human resource management. The outcomes of the project inform policy makers and technology developers the factors important to the fairness of personnel selection. It also facilitates discussions about the use of machine learning in human resource management, by better connecting the empirical research of personnel selection with the technical design of fair machine learning algorithms.

Addressing Biases in Measurement of Self-Reported Privacy Constructs

Sponsored by Meta

Understanding people's expectations and experiences with privacy is a challenge. This project acknowledges the existence of bias in self-reported privacy concerns and develops computational techniques to disentangle various biases, so as to properly understand people's privacy expectations and experiences.

OTHER ONGOING GRANTS

LEARN MORE AT
[AMERICAN.EDU/KOGOD/
RESEARCH/CYBERGOV/](https://AMERICAN.EDU/KOGOD/RESEARCH/CYBERGOV/)

Situation-Aware Identification and Rectification of Regrettable Privacy Decisions

Funded by the National Science Foundation, 2018-2023

People today are faced with many data disclosure decisions in their daily interactions with mobile devices. Despite numerous efforts to help individuals make better privacy decisions, users still make mistakes and regret their privacy decisions. This project sponsored by NSF and directed by Heng Xu and Nan Zhang casts a fresh perspective on Privacy-by-Redesign by helping users revisit and rectify past privacy decisions.

Establishing and Boosting Confidence Levels for Empirical Research Using Twitter

Funded by the National Science Foundation, 2018-2022

Concerns about a reproducibility crisis in scientific research have become increasingly prevalent within the academia and to the public at large. This \$400K project sponsored by NSF and directed by Heng Xu and Nan Zhang examines the inconsistent handling of organic data among scholarly publications in social and behavioral sciences, in order to assess the confidence (or the lack thereof) in the conclusions drawn from data analysis.

The Generalizability and Replicability of Twitter Data for Population Research

Funded by the National Science Foundation, 2018-2022

This \$500K project funded by NSF aims to evaluate the extent to which Twitter users represent the population across different demographic groups. Heng Xu, is a Co-Investigator, in collaboration with a group of social scientists at Penn State.



Research Highlights

A core mission of KCGC is to conduct world-class research on cybersecurity and privacy.

Privacy Protection and Disparity Detection

Research and practical development of data anonymization techniques has proliferated in recent years. Although the privacy literature has questioned the efficacy of data anonymization at protecting individuals against harms associated with re-identification, this paper raises another new set of questions: whether anonymization techniques themselves can mask statistical disparities and thus conceal evidence of disparate impact that is potentially discriminatory. If so, the choice of data anonymization technique to protect privacy, and the specific technique employed, may pick winners and losers. Examining the implications of these choices on the potentially disparate impact of privacy protection on underprivileged sub-populations is thus a critically important policy question.

The paper begins with an interdisciplinary overview of two common mechanisms of data anonymization and two prevalent types of statistical evidence for disparity. In terms of data-anonymization mechanisms, the two common ones are data removal (e.g., k-anonymity), which aims to remove the part of a dataset that could potentially identify an individual; and noise insertion (e.g., differential privacy), which inserts into a dataset carefully designed noises that block the identification of individuals yet allow the accurate recovery of certain summary statistics. In terms of the statistical evidence for disparity, the two commonly accepted types are disparity through separation (e.g., the "two or three standard deviations" rule for a prima facie case of discrimination), which is grounded in the idea of detecting the separation between the outcome distributions for different sub-populations; and disparity through variation (e.g., the "more likely than not" rule in toxic tort cases), which concentrates on the magnitude of difference between the mean outcomes of different sub-populations.

We develop conceptual foundation and mathematical formalism demonstrating that the two data

[View more at american.edu/kogod/research/cybergov/](https://american.edu/kogod/research/cybergov/)

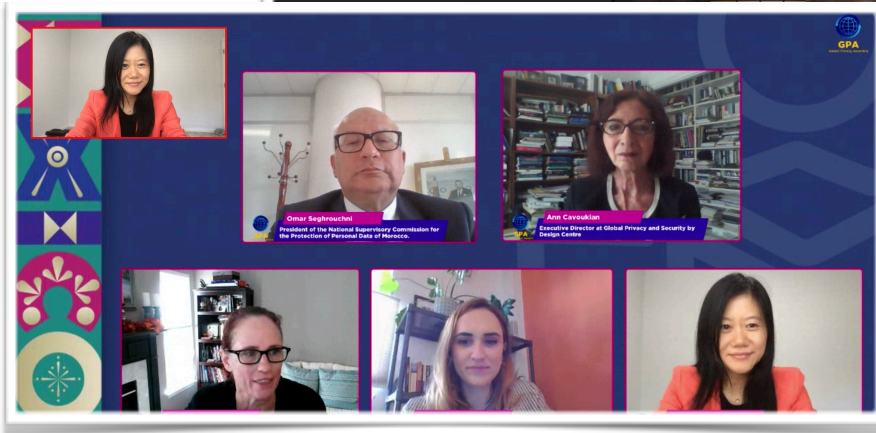
anonymization mechanisms have distinctive impacts on the identifiability of disparity, which also varies based on its statistical operationalization. Specifically, under the regime of disparity through separation, data removal tends to produce more false positives (i.e., detecting false disparity when none exists) than false negatives (i.e., failing to detect an existing disparity); while noise insertion rarely produces any false positives at all. Meanwhile, noise insertion does produce false positives (equally likely as false negatives) under the regime of disparity through variation; while the likelihood for data removal to produce false positives and false negatives depend on the underlying data distribution.

We empirically validated our findings with an inpatient dataset from one of the five most populated states in the U.S. We examined four data-anonymization techniques (two in the data-removal category and the other two in noise insertion), ranging from the current rules used by the State of Texas to anonymize their state-wide inpatient discharge dataset to the state-of-the-art differential privacy algorithms for regression analysis. After presenting the empirical results, which confirmed our conceptual and mathematical findings, we conclude the paper by discussing the business and policy implications of these findings, highlighting the need for firms and policy makers to balance between the protection of privacy and the recognition/rectification of disparate impact.

In sum, our paper identifies an important knowledge gap in both tech and law fields: whether data anonymization technologies themselves can mask statistical disparities and thus conceal the evidence of disparate impact that is potentially discriminatory. The emergence of privacy laws (e.g., GDPR) gives primacy to answering this question, because if such disparate impacts do exist, legislators and regulators would be essentially picking winners and losers by requiring or incentivizing the use of data anonymization techniques. This paper tackles this timely yet complex challenge, especially given the current public discourse in the U.S. about racial discrimination, and the worldwide trend of prioritizing the protection of consumer privacy in legislations and regulations.



From top: 1) Nan Zhang giving an invited talk about fairness of ratemaking for catastrophe insurance. 2) Heng Xu speaking at the Environmental, Social, and corporate Governance (ESG) symposium hosted by the University of Albany. 3) Heng Xu speaking about privacy research at the Global Privacy Assembly.





◀ IN THE PRESS

MARCH 2021

Continuing collaborations with the SANS Institute, KCGC provided all data cleaning and analytics support for the annual data-driven report on the state of the cybersecurity awareness training programs across industry sectors in the US and beyond.

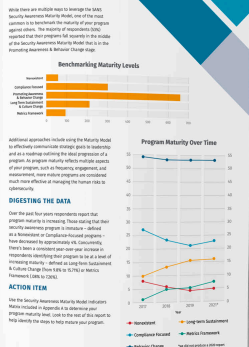
◀ IMPORTANCE TO KOGOD STUDENTS

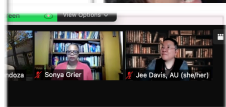
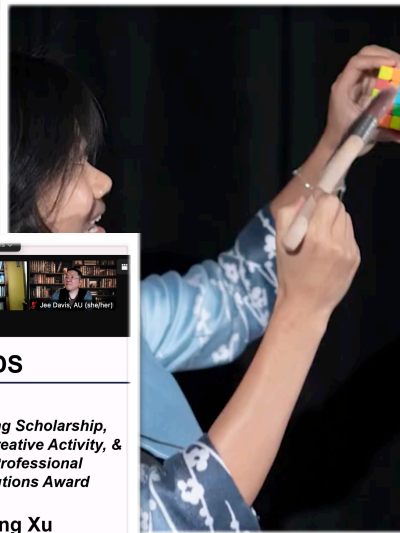
This year's report, titled "managing human cyber risks", notes that cybersecurity awareness training programs in a wide variety of organizations have grown considerably over the past few years, transitioning from a narrow focus on compliance to a broader mission of managing human cyber risks.

The report further presents three main findings. First, the top challenge facing cybersecurity awareness programs is time rather than budget.

Second, strategic alignment is important for the success of cybersecurity awareness training. Specifically, a key recommendation is to make security awareness teams an extension of the security team rather than as part of legal, audit, or human resource departments.

Finally, there is a lack of program leads with both technical issues and communication/marketing skills. This makes it challenging for many organizations to communicate cybersecurity-related issues in easy-to-understand terms to their workforce. This final finding suggests an attractive potential career for Kogod students to consider.



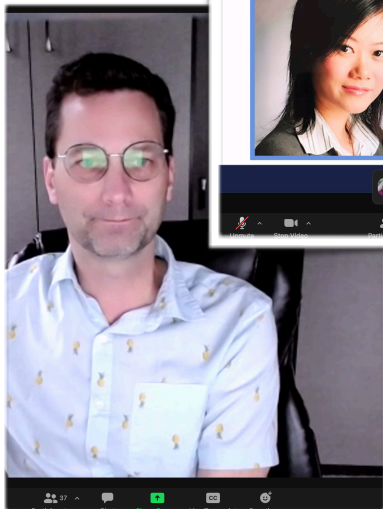


AWARDS

*Outstanding Scholarship,
Research, Creative Activity, &
Other Professional
Contributions Award*

Heng Xu

Information Technology and Analytics
Kogod School of Business



INFORMATION TECHNOLOGY AND ANALYTICS GOVERNANCE CENTER (KCGG)

**Class:
Managing Cyber Risks in
Supply Chain**

PM | Oct 13, 2020



Adeb Mahmoed

Senior Director of Cybersecurity Governance
Deputy Chief Cybersecurity Officer
Siemens USA



Jay Simon

Associate Professor of IT & Analytics
Faculty Fellow KCGG
Kogod School of Business

Business Focus:
Human Capital
Data Science
Risk Assess
**Kogod
Cybersecurity
Governance
Center**



SEMINARS AND EVENTS WITH STUDENTS AND ALUMNI

Top left: Dr. Heng Xu, President Sylvia Burwell, and Vice Provost for Research Diana Burley in an alumni engagement event "Change Can't Wait" in San Francisco, CA

Bottom left: Mr. Michael Daly, Vice President & Chief Information Security Officer at Vertex Pharmaceuticals and Chair of KCGC Advisory Committee, serving as a judge for the capstone projects of Kogod MS analytics students before speaking to students about a career in cybersecurity and analytics.

Center: Annual award celebration, American University

Top right: Dr. Heng Xu explaining our findings in AI fairness in alumni engagement event in San Francisco, CA

Bottom right: Mr. Adeeb Mahmood, Head of Americas Cybersecurity Defense Operations at Siemens, and Dr. Jay Simon, Faculty Fellow of KCGC, speaking to Kogod students about management cyber risks in the supply chain.



Research Workshop: Navigating the Human-AI Frontier

Intelligent, interactive, and highly networked machines -- with which people increasingly interact -- are becoming a growing part of our social landscape in both work and life. In order to define the key challenges and research imperatives for the nexus of human-AI interactions, it is important to promote the convergence of multiple disciplines -- in social and behavioral sciences, business research, computer science and engineering. To promote this vision, KCGC hosted a workshop that convened thought leaders in business research to share their perspectives and brainstorm a research roadmap for AI governance and the future of human-AI frontier. (See <https://robustanalytics.org/convergence2022/> for more details)

TH

In order to pursue world-class research on cybersecurity and privacy, KCGC relies on the support from Kogod leadership and our sponsors listed on the next page.

AN

We are very grateful for their extremely generous support, which enabled the many initiatives described in the report.

KY

OU

Any opinions, findings, and conclusions or recommendations expressed in this report and any other material published by the Center or its members are those of the author(s) only and do not reflect the views of the sponsors.



WARNER BROS.
DISCOVERY




Raytheon

amazon

Marriott
INTERNATIONAL

Meta

FINRA

A decorative graphic on the left side of the slide. It features a thin white curved arrow pointing downwards and to the left. Below the arrow is a thin white parallelogram. To the right of the parallelogram, a thin white horizontal line extends across the slide, ending in a small circle. On the far left, there is another small circle. On the far right, there is a larger circle with a crosshair inside it.

Biennial Report 2020-2022

Kogod Cybersecurity Governance Center (KCGC)

Kogod School of Business | American University | Washington, DC 20016

Contact: Prof. Heng Xu (Director) | cybergov@american.edu | 202.885.1832