2201 Crescent Pointe Parkway, Apt. 4302
College Station, TX 77845
m: +1 517 214 1900
e: jesse.sowell@gmail.com

Department of Science, Technology, Engineering, and Public Policy
University College London

Dear Faculty Search Committee,

I am writing to express my interest in the position of Lecturer in the Department of Science, Technology, Engineering, and Public Policy (STEaPP) at University College London. I am currently an Assistant Professor of International Affairs in the Bush School of Government and Public Service at Texas A&M University. My interdisciplinary PhD in Technology, Management, and Policy from MIT's Engineering Systems Division combines computer science, international political economy, and operations strategy. I believe integrated research, engagement, and teaching is key to understanding contemporary and emerging challenges facing Internet infrastructure governance and security, and for developing the next generation of policy analysts and researchers that contribute to solving global challenges such as cybercrime, platform governance, and improving Internet infrastructure in developing regions. My research provides significant insights into the politics of the epistemic communities managing the Internet's infrastructure and security, and the implications for integrating these untapped resources into evidence-based policy making and the global governance system. Over the past ten years, my engagement with these communities has created regional and global impact, including developing of cybersecurity communities in developing regions and addressing cybersecurity data governance challenges. In the last four years my teaching has integrated this work into a comprehensive, research-led cyber policy programme, blending theory, case studies, and innovative teaching methods to *(1)* develop students' critical thinking skills *(2)* applied to project-based deep dives into substantive domains that *(3)* that hones the skills necessary for policy analysts and researchers to bridge the gaps between policy and technical communities.

I believe my current and emerging research, upcoming policy engagement, and well-developed cyber policy curriculum is exceptionally well-suited to STEaPP and the Digital Technologies Policy Lab (DTPL). My current research complements existing work on infrastructure (McCarthy sp?), development (Julius and Jakub), and abuse (Tanczer). I believe my emerging work on co-regulatory approaches to combating disinformation and data governance would be a substantive contribution to the DTPL. I explicitly designed my cyber policy curriculum for social scientists from diverse intellectual backgrounds. The introduction to cyber policy and data science courses can easily be adapted for an undergraduate curriculum; my advanced courses on platforms and politics, and the advanced cyber course would appeal to students in the digital route and doctoral students. The DTPL and the Policy Impact Unit would ideal homes for programmes I am planning with industry and non-profit partners on cybersecurity data governance and the ongoing challenges facing collaborations between technical communities and law enforcement. I believe my intrinsically interdisciplinary portfolio is a rare and valuable complement to STEaPP's mission and programmes, and I would be absolutely thrilled at the opportunity to join your department.

Research

My research strategy has always been interdisciplinary. I started my academic life in computer science as a software engineer, focusing on programming languages and network security, but soon realized technical knowledge alone was insufficient to understand the complex sociotechnical dynamics shaping Internet development and cybersecurity challenges. My doctoral research at MIT combined international political economy, operations strategy, and computer science to conduct extensive fieldwork examining on-the-ground practices in Internet infrastructure management and cybersecurity. I funded the last year of my dissertation work as the primary author on a Google Faculty Research Award ($85,000).

As a Postdoctoral Cybersecurity Fellow at Stanford, I won two grants (totaling $125,000) evaluating the informal collaboration between global cybersecurity communities and law enforcement. I developed and executed the research plan, managed budgets and research assistants; and ran workshops and focus groups bringing together cybersecurity professionals, law enforcement, lawyers, and policymakers in the US, Africa, and Europe. The cumulative *Combined Capabilities* report evaluated these collaborations in terms of credibility and legitimacy norms within these groups and in the broader global governance system. In collaboration with colleagues at the Shadowserver Foundation, we are continuing this work in a report for Europol. This report documents and evaluates the technical, legal, and coordination learnings from the Avalanche botnet takedown, one of the largest concerted applications of Mutual Legal Assistance Treaties (40 jurisdictions).

My research has three common themes: *(1)* the coproduction of expert knowledge, *(2)* how it facilitates the adaptation necessary to keep pace with changes in technology and emerging security threats, and, *(3)* importantly, how to integrate expert knowledge into policy development, regulatory design, and global governance processes. My chapter on planned adaptation presents a generalized model for evaluating ad hoc and systemic planned adaptation in the regulation of complex engineering systems. In collaboration with Dr. I. Brass, our article in *Regulation & Governance* presents a planned adaptive regulatory framework for IoT security regulation and standards. My article in the *Journal of Cyber Policy* comparatively evaluates consolidation in digital platforms, highlighting how governance and accountability strategies employed by communities in the Internet's infrastructure preclude the predatory practices typically associated with platform consolidation. In an article currently under review with International Organization (included as a writing sample), I contribute to the literature on epistemic communities by empirically evaluating how institutions coordinating the Internet's infrastructure, in the absence of state regulation, accrued authority, and how to more effectively integrate these authorities into the broader global governance system. I believe my common research themes are exceptionally aligned with STEaPP's mission to mobilise deep expertise in complex engineering systems and policy to solve wicked global policy problems.

To coordinate across funded research projects, I created and fund the Internet Infrastructure and Policy Research Group (IIPRG), where I supervise four masters-level student researchers. IIPRG projects include *(1)* the politics and governance of submarine cables critical to Internet communication; *(2)* mix-methods modeling of the relationship between types of autocracy and Internet shutdowns, with technology transfer as an intervening variable; *(3)* studies of Internet infrastructure development in developing regions, with a special focus on Africa and Latin America; and *(4)* multilevel network analyses (combining organizational and individual ties) evaluating the globally diverse institutional complex that ensures the stability, safety, and security of the Internet, with a special focus on identifying gaps between this dense institutional network and the broader global governance system. The submarine cables work has produced one student-authored publication in the Journal of Policy and International Affairs, co-authoring a second that is under review by Contemporary Security Policy. My co-authored five-case piece on autocracies and Internet shutdowns is under review by the Journal of Peace Research, with a second using hierarchical clustering to further test our model on shutdown data from 2016 to 2021 in progress. I believe these research streams would not only benefit the DTPL, contributing additional novel and impactful research, but would also create fruitful linkages with the infrastructure and development research clusters. In addition to these work streams, through my engagement discussed below, I am developing new research streams on data governance and disinformation. Interdisciplinary research environments are my native habitat, and I am excited at the prospect of collaborating with colleagues in STEaPP and the DTPL on these projects.

Engagement and Impact Through Science Diplomacy

My deep, novel research findings would not be possible without continuous and trusted engagement with the epistemic communities managing the Internet's infrastructure and security. In the last ten years I have interviewed over 100 actors across these communities, at over 40 network operations and cybersecurity conferences around the world. Since completing my PhD, my engagement is best categorized as impact-driven science diplomacy. By demonstrating I speak technical, political, and business vernaculars, I have established a reputation as a trusted honest broker that brings a deep understanding of the complex, sociotechnical governance and management problems endemic in establishing collaborative engagement between these transnational institutions, policy makers and regulators, and law enforcement. I have developed rare (and hard won) access to diverse formal and informal institutions critical not only to combating cybercrime, but that also provide the access and empirical evidence necessary to developing rich, theory-based understandings of the kinds of collaboration necessary for keeping pace with continuous innovation by cybercriminals.

As a research fellow and advisor to the Anti-Phishing Working Group (APWG), I chaired the 2018 Symposium on the Policy Impediments to e-Crime Data Exchange, bringing together cybersecurity experts, lawyers, and policy-makers to highlight the GDPR as an opportunity to resolve the tensions between operational security groups, advocacy groups, and data protection authorities wrestling with tensions between privacy and security challenges. APWG's Secretary General Peter Cassidy recently shared that a number of participants from the 2018 Symposium indicated it was one of the most impactful meetings they have attended. This year we are continuing this work, planning an annual series of Cybersecurity Data and Governance Symposia to kick off in November 2022. Also with the APWG (in collaboration with Dr. L. Weissinger at Tufts' Fletcher School of Global Affairs) we evaluate the perverse incentives created by ICANN's ill-conceived GDPR compliance. The research findings will contribute to a collaboration with Senator Ed Markey's (D, MA) staff to develop model legislation to ensure the accessibility of data critical to cybersecurity incident response.

As a senior advisor to the Messaging, Malware, and Mobile Anti-Abuse Working Group (M^{3}AAWG), starting in 2016 I worked with the M^{3}AAWG Board to redesign their Outreach initiatives, creating and leading programs developing anti-abuse capabilities and capacity in Latin America and the Caribbean, Asia Pacific, and Africa, considering each regions' culture, values, and resource endowments, including critical support for engagement with regulators, law enforcement, and international organizations. I am also the co-chair of M^{3}AAWG's IoT Special Interest Group (SIG), working with Internet Service Providers (ISPs) to understand and evaluate the feasibiliy of IoT reputation models. I have included reference letters detailing these engagements from APWG and M^{3}AAWG leadership in the supporting documents.

Working with global partners in the cybersecurity, law enforcement, and policy communities, I apply my research on collaboration and governance to the development of impactful organizations that continue to develop cybersecurity capabilities and capacities in developed and developing regions. This engagement provides unique insights critical to my work. Understanding the real-world challenges of developing these collaborations provides rare, valuable, and pragmatic empirical evidence for both theory- and policy-relevant research contributions. On-the-ground work also provides unique perspectives into the diverse cultural and regional challenges facing Internet infrastructure development and security. These insights facilitate both impactful, responsible engagement and contribute significantly to my research-led teaching.

Teaching

Understanding the social, political, and economic challenges presented by emerging trends in Internet operations, operational cybersecurity, online platforms, and cybercrime requires engaging students in contemporary, real-world problems. I am a fourth generation teacher—a passion and dedication to teaching is in my nature. My pedagogy uses innovative teaching methods such as flipped classroom, peer review, and intensive dialog structured to encourage respectful, yet rigorous policy debates. In my Fall 2021 course evaluations, one student wrote:

> This is the first time I had Dr. Sowell and I felt he did a great job of explaining complex topics to a diverse audience. I was nervous to take a class without a STEM background but this class reaffirmed my decision and prepared me for other cyber courses I'm taking in the future. He genuinely cared about students learning the material and fostered critical thinking and discussion.

In my current role I designed, developed, and deliver, from scratch, my department's Cyber Policy Concentration (CPC)[1] from the ground up, offering a comprehensive curriculum and development programme for masters students coming from diverse disciplinary backgrounds. This interdisciplinary, research-led programme (now in its third year) provides accessible deep dives into digital technologies and the politics of these complex systems' design, operations, and security.

I developed and teach four of the five courses in the CPC:

Introduction to Cyber Policy Internet technologies foundations; longstanding issues such as attribution and encryption; contemporary issues such as privacy/surveillance and disinformation

Data Science and Visualization for Policy Analysis exploratory data analysis (clustering, social network analysis, text mining) and visualization for mixed methods hypothesis generation

Internet Infrastructure: Platforms and Politics deep dive into the institutional and infrastructure economics of online platforms and infrastructures

Advanced Cyber Policy evaluates the diverse complex of institutions shaping Internet governance through the lens of political authority and a systems approach to global governance

I have also led capstones engaging with the National Cyber Forensics Training Alliance (NCFTA) and the FBI.

Over the last four years I contributed to STEaPP's teaching portfolio with guest lectures in Risk & Regulation and Digital (need the full name). I am familiar with STEaPP's curriculum and course structure, and would love to work with STEaPP colleagues to integrate my courses into the Digital route's educational experience and identify cross-over topics with other routes. The first two above can easily be scaled to advanced undergraduate courses (syllabi included in supporting documents); the latter are appropriate for advanced MPA students and can be adapted for doctoral students. I am also keen to contribute to STEaPP's cumulative group projects. In addition to my relationships with law enforcement such as the FBI and Europol, I also have extensive relationships with organizations such as the Cyber Defense Alliance (CDA, based in London) and the Global Cyber Alliance (GCA, offices in London) that would be excellent partners for student projects in the Digital Route.

[1] Concentrations are similar to MPA routes in STEAPP. Our two-year masters requires students to complete two (optionally three) concentrations to graduate.

I am quite excited at the prospect of bringing my ongoing research projects, teaching, access to expert networks, and engagement initiatives to STEAPP. Please do not hesitate to contact me at jesse.sowell@gmail.com or +1 517 214 1900 with any questions about this application. Thank you for your time and interest, I am looking forward to hearing from you.

Sincerely,

Jesse H. Sowell II